

# **Navy Marine Corps Intranet (NMCI)**

## **Security Policy**

March 2000~~December 1999~~

Prepared for:

Department of the Navy  
Space and Naval Warfare Systems Command  
Naval Information Systems Security Office, PMW 161  
San Diego, CA

## 1.0 SYSTEM SECURITY POLICY

This security policy is a living agreement among the NMCI Program Manager, the Designated Approving Authority, Certification Authority, and the NMCI User Representative on the level of security required for the NMCI. The security policy supports the five fundamental information assurance elements (confidentiality, integrity, availability, authentication and non-repudiation) and establishes how the NMCI will manage, protect, and distribute sensitive information. The directive case (DC) security policy statements are derived from DoD and DoN directives and instructions to which the NMCI must adhere by virtue of its existence as a DoN information system. The mission case (MC) security policy statements counter vulnerabilities identified during the conceptual risk assessment.

### 1.1 Directive Cases

~~The NMCI security policy statements are derived from Presidential Decision Directives (PDD) 63, PDD 67, DoD Directive 5200.28, DoD 5200.28 STD, CJCSI 6510.01B (U) Defense Information Operations 22 AUG 97, CJCSI 6510.01B CH 1(U) Defense Information Operations, 26 AUG 98, SECNAVINST 5239.3, SECNAVINST 5510.36, OPNAVINST 5239.1B, DoD CSC-STD-002-85, DoN Information Technology Standards Guidance, DoD Information Technology Security Certification and Accreditation Process DoDI 5200.40 and DoD CIO Guidance Memorandums on Information Assurance (IA) 6-8510.~~

The NMCI security policy statements are derived from Presidential Decision Directives (PDD) 63, PDD 67, Department of Defense Critical Infrastructure Protection Plan of 18 November 1998, DoD Directive 5160.54 (Critical Infrastructure Protection) DoD Directive 5200.28, DoD 5200.28-STD, CJCSI 6510.01B (U) Defense Information Operations 22 AUG 97, CJCSI 6510.01B CH 1(U) Defense Information Operations, 26 AUG 98, SECNAVINST 5239.3, SECNAVINST 5510.36, OPNAVINST 5239.1B, DoD CSC-STD-002-85, DoN Information Technology Standards Guidance, DoD Information Technology Security Certification and Accreditation Process DoDI 5200.40 and DoD CIO Guidance Memorandums on Information Assurance (IA) 6-8510.

**SP-DC1** The NMCI shall take into account the objectives of the DoN Critical Infrastructure Protection Program and its guiding policies:

**SP-DC1-1** Department of Defense Critical Infrastructure Protection Implementation Staff Execution Plan

**SP-DC1-2** Department of Defense Critical Infrastructure Protection Plan of 18 November 1998.

**SP-DC1-3** Department of Defense Directive 5160.54, Critical Infrastructure Protection.

## NMCI Security Policy

~~The NMCI security policy statements are derived from Presidential Decision Directives (PDD) 63, PDD 67, DoD Directive 5200.28, DoD 5200.28-STD, CJCSI 6510.01B (U) Defense Information Operations 22 AUG 97, CJCSI 6510.01B-CH 1(U) Defense Information Operations, 26 AUG 98, SECNAVINST 5239.3, OPNAVINST 5239.1B, DoD CSC-STD-002-85, DoN Information Technology Standards Guidance, DoD Information Technology Security Certification and Accreditation Process DoDI 5200.40 and DoD CIO Guidance Memorandums on Information Assurance (IA) 6-8510.~~

**SP-DC1SP-DC2** The NMCI shall comply with the minimum Automated Information System (AIS) security requirements provided by DoD Directive 5200.28.

**SP-DC2SP-DC3** The NMCI shall comply with the applicable provisions of SECNAVINST 5239.3.

**SP-DC2-1SP-DC3-1** Data processed, stored and transmitted by DoN information systems shall be adequately protected with respect to requirements for confidentiality, integrity, availability and privacy.

**SP-DC2-2SP-DC3-2** All DoN information systems shall be protected by the continuous employment of appropriate safeguards.

**SP-DC2-3SP-DC3-3** Classified information processed or stored by DoN information systems shall be safeguarded as required by that level of classification.

**SP-DC3SP-DC4** The NMCI shall incorporate required boundary protection mechanisms to properly segregate systems operating at different classification levels. As required by national policy (DODD C-5200.5), all U.S. classified information must be protected with National Security Agency (NSA) approved high-grade cryptography.

**SP-DC5** The NMCI shall comply with the applicable provisions of SECNAVINST 5239.3 and SECNAVINST 5510.36.

**SP-DC5-1** Data processed, stored and transmitted by DoN information systems shall be adequately protected with respect to requirements for confidentiality, integrity, availability and privacy.

## NMCI Security Policy

**SP-DC5-2** All DoN information systems shall be protected by the continuous employment of appropriate safeguards.

**SP-DC5-3** Non-Classified and Classified information processed or stored by DoN information systems shall be safeguarded as required by that level of classification.

~~SP-DC4~~The NMCI shall be certified and accredited in accordance with DITSCAP procedures outlined in DoD Information Technology Security Certification and Accreditation Process DoDI 5200.40.

**SP-DC5****SP-DC6** The NMCI shall comply with NSTISSAM TEMPEST/2-95, "RED/BLACK Installation Guidance" of 12Dec95 and NAVSO P-5239-22, "Protected Distribution Systems (PDS) Guidebook" of Oct 97 for TEMPEST requirements.

**SP-DC6****SP-DC7** The NMCI shall comply with SECNAVINST 5510.30A, "Department of the Navy Personnel Security Program" of 10 Mar 99 and SECNAVINST 5510.36 Department of the Navy Information Security Program Regulation" of 17 Mar 99, which provide regulations and guidance for classifying and safeguarding information. Communications security (COMSEC) information shall be handled and controlled in accordance with national and departmental directives.

**SP-DC7****SP-DC8** The NMCI shall implement password control systems in accordance with CSC-STD-002-85, DoD Password Management Guideline, dated 12 April 1985.

**SP-DC8****SP-DC9** The NMCI shall comply with the policy, guidance, standards, and best practices from Chapter 3 of the Information Technology Standards Guidance, 5 April 1999, published by the DoN Chief Information Officer.

**SP-DC8-1****SP-DC9-1** Content security checking mechanisms to scan for malicious code shall be implemented by the NMCI and all connecting networks, systems and subsystems.

**SP-DC9****SP-DC10** The NMCI shall comply with the DoD CIO Information Assurance Guidance and Policy Memorandum – 6-8510 (Draft) requirement for the appropriate level of robustness.

**SP-DC9-1****SP-DC10-1** All NMCI information systems shall be monitored to detect, isolate, and react to intrusions, disruptions or denials of services, or other incidents that threaten the security of the NMCI.

~~SP-DC9-2~~SP-DC10-2 The NMCI shall follow an enterprise-wide IA architecture that implements a defense-in-depth (DiD), notionally depicted in figure 1. The DiD approach shall incorporate multiple protection schemes at different levels to establish and maintain an overall acceptable IA posture across the NMCI. These boundaries are:

- Boundary 1: Logical Boundary between NMCI and External Networks.
- Boundary 2: Logical Boundary between NMCI and Communities of Interest (COIs). These COIs could be at Metropolitan Area Network (MAN)/Base Area Network (BAN)/Local Area Network (LAN) level, or between different organizations or functional groups.
- Boundary 3: Logical Boundary between COIs and Host level I.
- Boundary 4: Final Layer of Defense: Application/Host Level.

~~Proposed~~NMCI Boundary One and Two-NIPRnet and SIPRnet Firewalls shall conform to policy referenced in NMCI Security Requirements Document, paragraph 1.2.3 and paragraph 1.2.4.

Corresponding to the discussion of boundaries within the NMCI is a discussion of layers of defense implemented as part of a Defense in Depth strategy. The number of layers of defense protecting any given network node will depend on its physical placement within the NMCI architecture, criticality in support of warfighting capabilities, and restrictions on data or protocols at the node.

If properly designed, carefully deployed, securely configured, and regularly maintained, the Defense in Depth strategy can significantly enhance the security posture of the DoN's information infrastructure, and ensure that the information it provides to the warfighter is appropriately protected, accurate, and timely, and that the data and communications channels essential to command are instantly, and always, accessible. Such protections play a critical role in establishing and maintaining the DoN's information superiority, and effect the speed of command that is vital to our warfighting capability.

Additional and more detailed information describing the Defense in Depth strategy, protection mechanisms, and current policy and standards can be found in the ITSG document and the Network Defense Strategy document titled "NMCI Active Computer Network Defense Strategy: Cyber-Centric Maneuver Warfare" Additionally, SPAWAR PMW 161, the Navy's INFOSEC organization, maintains a web page

## NMCI Security Policy

(<http://infosec.navy.mil>) with comprehensive links to INFOSEC information, including information on available security products, links to anti-viral tools, INFOSEC news and articles, security policies and procedures, and the Naval Computer Incident Response Team (NAVCIRT).

~~With respect to Layers of Defense, within the NMCI there will be applicable security policies that will be implemented at various layers. Based on the boundaries defined earlier, it is envisioned that the following layers will be applicable for NMCI security policy implementation.~~

- Layer 0: Demilitarized Zone (DMZ). This would affect communication between the NMCI and public networks that is not afforded the same degree of protection provided by an integrated network security suite.
- Layer 1: External boundary level protection. This would affect communication between the NMCI and external networks such as NIPRnet/INTERNET or SIPRnet.
- Layer 2: Communication internal to the NMCI.
- Layer 3: Communication within COIs in the NMCI without the use of a VPN
- Layer 4: Communication within COIs in the NMCI with the use of VPN
- Layer 5: Application/Host Level.

~~Within the various boundaries and layers of defense within the NMCI, applicable security policies will be implemented. The NMCI Governance and Operations Organization shall be responsible for the implementation of these security policies. The above noted boundary 1 firewall policies are a subset of these security policies. NMCI layers 1 and 2 NIPRNet and SIPRNet firewalls shall perform to policy referenced in NMCI Security Requirements document paragraphs 1.2.3 and 1.2.4.~~

## NMCI Security Policy

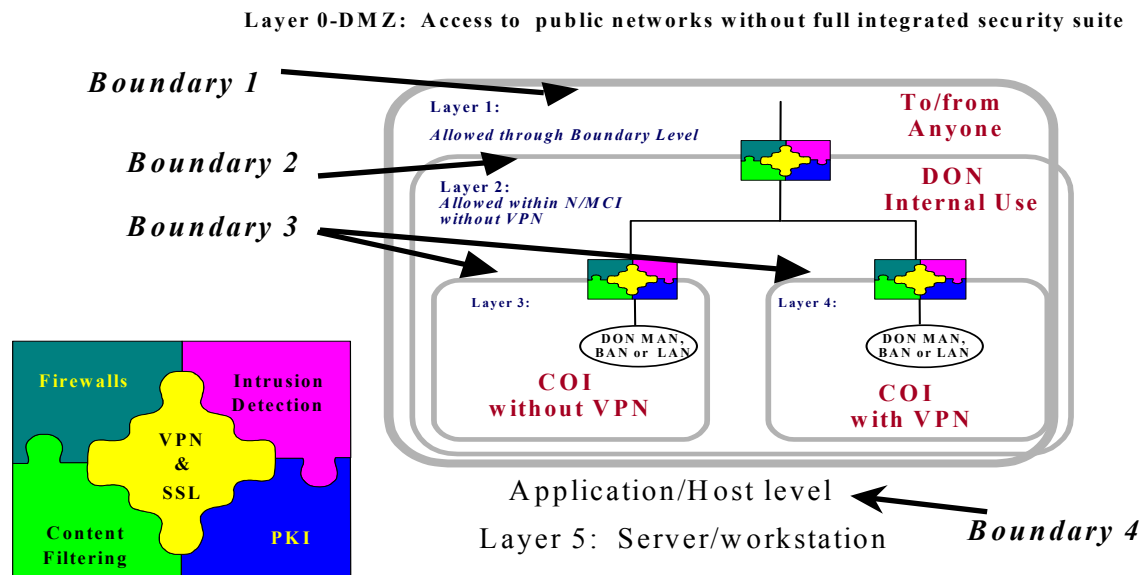


Figure 1. NMCI Notional Security Layer Architecture

**SP-DC10SP-DC11** NMCI information systems using Windows NT 4.0 should be configured according to guidance documented in "Secure Windows NT Installation and Configuration Guide", SPAWAR PMW-161 report, December 1998 and May 1999.

**SP-DC11SP-DC12** The NMCI shall comply with DISN security policy and DISA requirements for connection to the SIPRNET, dated 20 August 1998.

**SP-DC12SP-DC13** Use of a Public Key Infrastructure (PKI) within NMCI shall be DOD PKI in accordance with NMCI Security Requirements document. ~~Use of a Public Key Infrastructure (PKI) within NMCI shall be DOD PKI in accordance with DEPSECDEF Memo dated 9 April 1999.~~

**SP-DC14** Virtual Private Network (VPN) devices used within NMCI shall be selected in accordance with NMCI Security Requirements Document.

~~SP-DC13 Virtual Private Network (VPN) devices used within NMCI shall be selected according to Naval VPN Selection Criteria document dated 18 November 1999.~~

## NMCI Security Policy

**SP-DC14SP-DC15** NMCI shall be able to support the communities of interest defined in paragraph 1.2.1.9 of the NMCI Security Requirements document.

**SP-DC15SP-DC16** Security services provided for/within the NMCI shall implement CND initiatives such as Information Operations Condition (INFOCON) directives, and Information Assurance Vulnerability Alert (IAVA) notices, and shall be integrated within the existing DoD and DoN CND infrastructure.

**SP-DC16SP-DC17** Implementation of NMCI shall be consistent with current DoN Computer Incident Reporting guidelines such as OPNAVINST 2201.2, dated 3 Mar 98, Navy and Marine Corps Computer Network Incident Response.

**SP-DC17SP-DC18** Network availability and security sensor information from the entire NMCI shall be made available to DoN CND components (FIWC, NCTF-CND MARCIRT and MARFOR-CND).

**SP-DC18SP-DC19** DoN components (NCTF-CND and MARFOR-CND) of JTF-CND shall work with other elements of JTF-CND to coordinate NMCI network defense across DoD and the U.S. Government as a whole.

**SP-DC20** The NMCI shall comply with the National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11 for ~~thee implementation~~ ~~acquisition~~ of COTS and GOTS IA and IA-enabled IT products.

**SP-DC20-1** Preference will be given to COTS IA and IA-enabled IT products evaluated and validated, as appropriate, in accordance with one of the following:

- The International Common Criteria for Information Security Technology Evaluation Mutual Recognition Arrangement;
- The National Security Agency (NSA)/National Institute of Standards and Technology (NIST) National Information Assurance Partnership (NIAP) Evaluation and Validation Program; or
- The NIST Federal Information Processing Standard (FIPS) validation program.

**SP-DC19-2 20-2** By 1 July 2002, the ~~implementation~~~~acquisition~~ of all COTS IA and IA-enabled IT products ~~to be used within the NMCI on the systems specified in paragraph (6), above,~~ shall be limited only to those which have been evaluated and validated in accordance with the criteria, schemes, or programs specified in the ~~three sub-bullets~~ of ~~SP-DC19-1~~.

**SP-DC2019-3** The acquisition of all GOTS IA and IA-enabled products to be used on systems entering, processing, storing, displaying, or transmitting national security information shall be



limited to products which have been evaluated by the NSA, or in accordance with NSA-approved processes.

## **1.2 Mission Cases**

Conceptual risk analysis of the proposed operation of the NMCI in the intended environment identified several vulnerabilities that could be exploited to seriously impair mission-critical system performance. This subsection delineates the mission case security policy statements that mitigate the associated risk.

**SP-MC1** All system operators shall receive thorough system training commensurate with user/administrator level. See attached System Administrators Training & Certification guidelines to determine specific qualifications and standards, this is in accordance with IA Training and Certification joint memo dated 29 June 1998, from Under Secretary of Defense (Personnel and Readiness) and Assistant SECDEF for C3I.

**SP-MC2** The NMCI shall adjust its security posture based on updated cyber threat and INFOCON status.

**SP-MC3** NMCI availability shall be independent of user action, either deliberate or accidental.

**SP-MC4** The NMCI shall be testing for obvious flaws that would allow violation of resource isolation or permit unauthorized access. All discovered flaws shall be removed or neutralized and the network re-tested to demonstrate that they have been eliminated and that new flaws have not been introduced.

**Attachment**

**System Administrators Training & Certification**

**Criteria for Coding U.S. Navy  
Systems Administrators and Maintainers**

September 13, 1999

This document contains excerpts from a Department of Defense (DoD) document issued January 9, 1998, under the title, "Information System Administrator Operations and Security Training: Training, Educating, and Licensing Department of Defense Systems Administrators."

**2.0 Purpose**

It is imperative the Department of Navy (DoN) understands and manages today's dynamic and growing information system processing infrastructure. Through various programs and policies, there are inordinate numbers of people performing tasks as *system administrators*. Some of these tasks can be performed with little knowledge while others require extensive training and experience. Results from the joint Staff's *Eligible Receiver '97* exercise revealed the need to assure consistent verifiable skill sets for individuals functioning as system administrators, primarily in support system security functions. This paper outlines three separate levels and maps skills against them so DoN managers can adequately train system administration personnel, thereby gaining more efficient operational use of them and assuring information system protection.

Commands will use the information in this paper as guidance to determine the appropriate level of each system administrator or maintainer position.

**Introduction**

Throughout this paper the term *system administrator* will be used. Commands may have various definitions of system administrators, but *in all cases* systems administrators are generalists. They install, tune, and maintain information systems and associated networks. System administrators:

- ☐ install and configure software
- ☐ teach users operational duties and solve operations-related problems,
- ☐ write scripts/programs
- ☐ repair or upgrade hardware,
- ☐ with Information System Security Officers, enforce security

Information System Security functions are primarily the responsibility of the Information System Security Officer (ISSO). With dwindling resources and ever decreasing manpower oftentimes the job of the system administrator and the ISSO blend into one. The INFOSEC functions of a system administrator are:

- ☐ working closely with the ISSO to ensure the information system or network is used securely.
- ☐ participating in the INFOSEC incident reporting program.
- ☐ assisting the ISSO in maintaining configuration control of the Systems and application software
- ☐ advising the ISSO of security anomalies or integrity loopholes, and
- ☐ administering, when applicable, user identification or authentication mechanisms of the information system or network.

### 3.0 System administrator levels

The break down of levels and tasks does not take into account the practice of specialization. In many organizations, systems administrators gravitate to becoming local experts in a specific topic (e.g., word processing, presentation applications, routers, and e-mail applications), often with no more experience than a Level 1 system administrator.

The term *domain* is used as a way to bound the focus, or realm of control, of any given information system management organization, regardless of the organization size.

### 4.0 Level 1

A level 1 system administrator is a novice with limited operational experience. Individuals coming from training organizations or recently graduating from service schools are considered *trainees* and reach level 1 status after a predetermined time of on-the-job training, but not normally sooner than one year on the job.

A healthy domain should have a steady supply of level 1 system administrators progressing to level 2.

### Tasks

Level 1 tasks should include:

- ☐ day-to-day operations such as backups, restores, adding/modify/deleting user accounts
- ☐ installing operating systems, applications and peripherals
- ☐ troubleshooting user problems
- ☐ debugging command language scripts
- ☐ assisting the ISSO in access control security (i.e., passwords, access and control lists, etc)

## Level 2

Level 2 systems administrators are the work-horses in a domain. They perform the majority of the daily tasks that keep a domain running smoothly. They are the expert technicians that can work simultaneously on several problems. The ultimate success of a domain is highly dependent on having a core group of level 2 system administrators. At least half of the system administrators in a healthy domain should be at level 2.

### Tasks

Level 2 tasks should include:

- ☐ taking the lead in solving day-to-day operational problems
- ☐ implementing complex operating system changes
- ☐ with ISSO, ensuring that established security mechanisms are functioning properly
- ☐ debugging operating system, application, and network problems
- ☐ following domain parameters, defining default environment for Systems for users
- ☐ maintain and enforce adherence to standards
- ☐ monitor and balance load among servers and networks within the domain
- ☐ interacting with developers, operations centers, and support personnel to maintain daily operations
- ☐ keeping the environment up and running smoothly

## Level 3

There are few truly experienced administrators. They have successfully separated themselves from the daily operations and concentrate on tasks that can be leveraged with their knowledge. Large domains should have one or two level 3 administrators leading the technical effort and setting the policy and direction for the domain. The absence of a level 3 tends to leave the *domain* with no clear *direction*.

### Tasks

Level 3 tasks should include:

- ☐ Taking general direction from management and turning it into a well thought out solution or design
- ☐ Setting and/or interpreting standards
- ☐ Planning and designing the architecture of their domain
- ☐ Working with the ISSM and ISSOs, planning security procedures, mechanisms, and architecture of their domain
- ☐ Tuning the performance of existing domains
- ☐ Solving the tough problems that others have not been able to fix
- ☐ Leading teams to tackle complex problems
- ☐ Teaching other system administrators
- ☐ Publishing guidance and lessons learned

## Level Recognition

## NMCI Security Policy

The requirements outlined at each level are rather subjective. Level recognition can be loosely based on an individual's status within existing information system career panel organizations. The below chart draws from the National Security Agency System Administration Specialty Job Task Analysis Map and cross-references recommended levels to job tasks.

NSA Mapping of Level to Job Task Analysis:

Level 3	Level 2	Level 1	Task
			<b>Manage System Hardware</b>
3			Plan hardware installation
3			Acquire hardware
3			Coordinate network installation
	2		Schedule preventative maintenance
	2		Coordinate hardware repair
		1	Install hardware
		1	Boot system
		1	Maintain inventory of system hardware
		1	Order consumable supplies
		1	Run diagnostics
		1	Relocate hardware
			<b>Manage System Software</b>
3			Optimize operating system parameters
3			Plan system changes
	2		Set system defaults
	2		Generate new operating system kernel
	2		Maintain system start-up and shutdown procedures
	2		Maintain command files
	2		Test validity of updates
		1	Install system software
		1	Shut down system

		1	Reboot system
		1	Maintain inventory of system software
		1	Install system changes
		1	Install vendor specific software
		1	Install system updates or patches
		1	Maintain documentation
			<b>Main Data Store</b>
3			Plan data storage layout
3			Plan backup procedures
	2		Implement backup procedures
	2		Monitor data storage utilization
	2		Maintain integrity of file system
	2		Audit file system security
	2		Delete unnecessary files
	2		Manage log files
	2		Maintain data storage layout
		1	Format media storage
		1	Partition disks
		1	Create a file system
		1	Load data

Level 3	Level 2	Level 1	Task
			<b>Manage Application Software</b>
3			Evaluate impact of software package
3			Optimize application parameters
3			Plan application changes
	2		Ensure compatibility among applications
	2		Allocate system resources to applications

	2		Validate integrity of applications before install
	2		Test validity of software installation
		1	Install application software
		1	Maintain inventory
		1	Maintain application documentation
		1	Install application updates
			<b>Provide Communication Connectivity</b>
3			Plan network configuration
	2		Request interhost connectivity
	2		Acquire internet address
	2		Build network tables
	2		Configure TTY lines
	2		Configure peripheral lines
	2		Configure file servers and clients
	2		Configure firewalls
	2		Monitor network activity
	2		Manage network services
	2		Manage network bridges and routers
	2		Manage print servers
	2		Manage network topology
		1	Assign addresses to node
		1	Install network software
		1	Set access permissions
		1	Start network software
		1	Test communication connectivity
		1	Stop network software
		1	Re-establish host connectivity
			<b>Ensure Security</b>

3			Help establish audit guidelines
3			Help establish user security guidelines
3	2		Assist writing system security plans
3	2		Assist in host network accreditation
	2		Ensure output labeling procedures
	2		Ensure data labeling procedures
	2		Assist testing security mechanisms
	2		Assist in analysis of audit trails
Level 3	Level 2	Level 1	Task
	2		Assist in incident handling
3	2	1	Enforce security procedures
		1	Assist in maintaining physical security for system

		1	Assist in maintaining device access controls
3	2		Report security incidents
			<b>Manage Accounts</b>
3			Plan account management strategy
	2		Establish user login environments
	2		Assist in managing mandatory access controls
	2		Manage account privileges
	2		Audit account activity
	2		Manage resources used by accounts
		1	Add new accounts
		1	Assist in setting account's access control list
		1	Explain basic operating procedures
		1	Assist in modifying passwords
		1	Delete accounts
			<b>Interact with Others</b>



3			Make recommendations to management
3	2	1	Coordinate with other system administrators
3	2		Participate in working groups
3	2		Present briefings
3	2		Delegate responsibilities
	2		Train users
	2		Generate working aids
	2		Interact with system support personnel
	2		Interact with hardware support personnel
	2		Interact with software developers
	2	1	Interact with vendors
3	2	1	Communicate with ISSM/ISSO
	2		Communicate with network operations centers
	2		Communicate with system operations centers
		1	Provide working aids
		1	Inform users of system status
		1	Handle user calls
			<b>Troubleshoot problems</b>
	2		Recreate scenario
	2		Interpret error messages
	2		Test components
	2		Isolate problems
	2		Maintain log of problems and solutions
	2		Recover from system crashes
Level 3	Level 2	Level 1	Task
		1	Respond to user identified problems
		1	Gather information
		1	Use diagnostic tools

		1	Initiate corrective action
3	2	1	<b>Maintain expertise</b>
3	2	1	Explore system capabilities
3	2	1	Interpret technical manuals
3	2	1	Attend classes
3	2	1	Participate in peer groups
3	2	1	Read journals
3	2	1	Attend seminars and conferences

## **System Administrator Level 1 Certification Criteria**

**System Administrator Level 1 Certification requires the following technical training, IA training, and on-the-job experience:**

- *Formal technical training equivalent to Level 1 Technical Training Minimum Standards<sup>1</sup>*  
**and**
- *Completion of Operational Information Systems Security CBT (2 vol.)*  
**and**
- **1 year System Administrator experience**

### **5.0 Notes**

#### **<sup>1</sup> Level 1 Technical Training Minimum Standards**

**Formal technical training in the following areas:**

- **microcomputer components and maintenance**
- **basic system troubleshooting**
- **computer networking fundamentals**
- **basic network protocols and operating parameters**
- **common system/network vulnerabilities**
- **basic Windows NT system concepts and operation**
- **basic UNIX system concepts and operation**

#### **Equivalent CNET Schools**

**RM “A” school graduates as of January 1996, CTO “A” school graduates as of August 1999, and CTM “A” school graduates as of August 1998.**

Equivalent NETg Technical Training Course of Instruction for Level 1

<b><u>Course #</u></b>	<b><u>Course Title</u></b>
<b>13114</b>	<b>A+ Certification PC Tech - Part 1</b>
<b>71441</b>	<b>MS Networking Essentials 2nd ed. - Part 1</b>
<b>71442</b>	<b>MS Networking Essentials 2nd ed. - Part 2</b>
<b>71006</b>	<b>MS Win NT 4.0 User Fundamentals</b>
<b>71401</b>	<b>MS Windows NT 4.0 Administering - Part 1</b>
<b>71402</b>	<b>MS Windows NT 4.0 Administering - Part 2</b>
<b>12327</b>	<b>UNIX Fundamentals</b>
<b>12426</b>	<b>UNIX Intermediate Topics</b>
<b>12258</b>	<b>TCP/IP Concepts and Architecture</b>

*Total of 9 classes, approximately 60 hours of instruction.*

**A+ Certification: PC Technologies - Part 1**

Course 13114

**LEARN TO:**

- Identify microcomputer components.
- Identify features and types of microprocessors.
- Describe bus structures.
- Identify the different types of memory that a microcomputer uses.
- Identify the characteristics of a portable computer, a Personal Digital Assistant, a Network Computer (NC), and a voice recognition device.
- Identify the various peripheral devices that are used with microcomputers.
- Identify the various methods and tools used for troubleshooting a microcomputer.
- Identify the various methods and tools used for preventive maintenance of a microcomputer.

**COURSE LENGTH:** 6 - 8 hour(s)

**Unit Names:**

Unit 1: Introduction to Microcomputers

Objectives:

- Identify the characteristics of a system unit.
- Identify the characteristics of a power supply device.
- Identify the components of a system board.
- Differentiate between the characteristics of serial and parallel ports in a microcomputer.
- Identify the factors that impact the performance of a microprocessor.
- Match the types of microprocessors with their features.
- Match types of buses with their functions.
- Identify the features of an expansion bus.
- Identify the features of a Peripheral Component Interface (PCI) bus.

- Identify the features of Personal Computer Memory Card Industry Association (PCMCIA) bus.
- Identify the characteristics of the Universal Serial (US) bus.
- Match the types of Read Only Memories (ROMs) with their descriptions.
- Differentiate between the two types of Random Access Memory (RAM).
- Match the various Dynamic Random Access Memory (DRAM) types with their functions.
- Identify the characteristics of a portable computer.
- Identify the characteristics of a Personal Digital Assistant.
- Identify the characteristics of a Network Computer.
- Identify the characteristics of a Voice Recognition Device.

## Unit 2: Peripheral Devices

### Objectives:

- Identify the features that are used to distinguish keyboard types.
- Identify the mouse positioning mechanisms that are used to position a cursor.
- Identify the principle on which a scanner converts an image into digital data.
- Identify the three ways in which a digitizer can position a cursor on the screen.
- Identify the factors that impact how a monitor works.
- Identify the features of different types of display adapters.
- Identify the functions performed by a modem.
- Match the types of modems with their features.
- Identify the components of a hard disk.
- Identify the factors that determine a hard disk's performance.
- Identify the features of standard hard disk interfaces.
- Identify the characteristics of a Redundant Array of Independent Disks (RAID) level.
- Identify the types of floppy disk drives.
- Identify the features used to distinguish between different floppy disks.
- Identify the features of a CD-ROM.
- Identify the features of a Write Once/Read Many (WORM) drive.
- Identify the features of a Digital Video Disk (DVD).
- Identify the recording standards for magnetic tape drives.

## Unit 3: Troubleshooting and Preventive Maintenance

Objectives:

- Match the troubleshooting tools used to troubleshoot a microcomputer with their descriptions.
- Identify the checks that must be performed to troubleshoot a microcomputer.
- Match the types of utilities that help in managing microcomputer software with their uses.
- Identify the measures that protect a PC from Electrostatic Discharge (ESD).
- Sequence the steps in discharging a Cathode Ray Tube (CRT).
- Identify the environmental conditions required for optimal system performance.
- Select the appropriate preventive maintenance procedure for a PC component.
- Identify the devices used to safeguard a PC from power-related problems.
- Identify the effect of different types of viruses on a PC.
- Identify the measures that safeguard a system from virus attacks.

**Networking Essentials 2nd Edition - Part 1**

Course 71441

*Produced by NETg*

**LEARN TO:**

- Identify the definition of networks and types of networks.
- Identify the characteristics of different approaches to networking.
- Identify the characteristics of different connecting components used for connecting computers.
- Select the appropriate connecting component in a given situation.

**COURSE LENGTH:** 6 - 8 hour(s)

**Unit Names:**

Unit 1: Network: Fundamentals

Objectives:

- Identify the type of a network for a given set of specifications.
- Match the elements of a network with their descriptions.
- Identify the benefits of using a network.
- Identify the characteristics of peer-to-peer networks.
- Identify the characteristics of server-based networks.
- Identify the characteristics of combination networks.
- Match the different types of specialized servers with the functions performed by them.
- Distinguish between peer-to-peer and server-based networks based on their advantages.
- Distinguish between share-level and user-level security on a server.
- Select the appropriate network approach for a given set of requirements.
- Identify the capabilities of a network that are affected by choosing one topology over the other.
- Identify the characteristics of bus topology.



- Identify the characteristics of the star topology.
- Identify the characteristics of ring topology.
- Identify the characteristics of the mesh topology.
- Distinguish between star bus and star ring hybrid topologies.
- Select the appropriate topology given a set of requirements.

## Unit 2: Connecting Network Components

### Objectives:

- Identify the characteristics of the primary cable types.
- Identify the type of twisted-pair cables to be used for a given network.
- Identify the benefits of the two types of coaxial cables.
- Identify the characteristics of the two types of fiber-optic cables.
- Identify the connecting hardware required to connect cables in a given network.
- Match the types of cables used in the IBM cabling system with their description.
- Identify the appropriate cable type for a given set of specifications.
- Identify the characteristics of the two techniques of signal transmission.
- Identify the uses of the three types of Wireless networks:

### Wireless LAN

### Extended LAN

### Mobile Computing

- Identify the transmission techniques used by wireless LANs in a given situation.
- Identify the characteristics of point-to-point transmission.
- Identify the signal transmission method used in a given situation for mobile computing.
- Identify the functions of a network adapter card.
- Match the configuration options for network adapter cards with their uses.
- Identify the devices causing the IRQ conflict with the network adapter card in a given situation.
- Identify the range of the Base I/O port settings for configuring a network adapter card.
- Select the network adapter card for a given situation.
- Match the methods with the enhancements to the network adapter cards for improved network performance.

**Networking Essentials 2nd Edition - Part 2**

Course 71442

*Produced by NETg*

**LEARN TO:**

- Explain the concepts and procedures related to the functioning of a network.
- Describe the characteristics of the four major network architectures: Ethernet, Token Ring, Apple Talk and ArcNet.

**COURSE LENGTH:** 6 - 8 hour(s)

**Unit Names:**

Unit 1: Network Functioning

Objectives:

- Match the layers of the OSI model with their functions.
- Identify the Project 802 enhancements to the OSI Model.
- Identify the role of network drives.
- Identify the purpose of driver interfaces.
- Install a network adapter card driver in a Windows NT Server-based computer.
- Remove a network adapter card driver from a Windows NT Server-based computer.
- Identify the advantages of using packets to transmit data over the network.
- Identify the information contained in a packet.
- Sequence the steps to transmit a packet.
- Identify the characteristics of packet switching.
- Sequence the steps performed by a protocol to transmit data over a network.
- Match the OSI stack protocol with the communication tasks that they perform.
- Identify the features of protocol types.
- Select the protocol that is best suitable for a given scenario.

- Implement a protocol on a Windows NT Server.
- Remove a protocol from a Windows NT Server.
- Identify the features of the CSMA/CD access method.
- Identify the features of the token passing access method.
- Identify the features of the Demand Priority access method.

## Unit 2: Network Architectures

### Objectives:

- Identify the features of the Ethernet network architecture.
- Identify the specifications of the 10 Mbps Ethernet topologies.
- Identify the features of 100 Mbps Ethernet topologies.
- Identify the features of a Token Ring network.
- Sequence the steps in the working of a Token Ring network.
- Match the hardware components of a Token Ring network with their functions.
- Identify the features of Apple Talk.
- Identify the features of ArcNet.
- Identify the guidelines for implementing a network architecture.
- Identify the network architecture for a given situation by using the network architecture selection checklist.

## **Microsoft Windows NT 4.0 User Fundamentals**

Course 71006

### **LEARN TO:**

- Perform tasks from the Desktop.
- Understand the basics of using Windows NT 4.0 Workstation.
- Use Explorer to view and manipulate files and folders in Windows NT Workstation.

**COURSE LENGTH:** 4 hour(s)

### **Unit Names:**

#### Unit 1: Using the Desktop

##### Objectives:

- Identify the features associated with Windows NT 4.0 Workstation.
- Log into Windows NT 4.0 Workstation.
- Change your password.
- Identify the purpose of My Computer, Network Neighborhood, Recycle Bin and My Briefcase.
- Utilize options available in the Accessibility Options dialog box to change system settings to make it easier to use Windows.
- Use the Add New Hardware utility to add devices to your PC.
- Change the default printer.
- Modify programs installed on the hard drive with the Add/Remove Programs utility.
- Identify options for arranging Desktop items.
- Create a shortcut on the desktop.
- Use the New Command in the Shortcut menu to create a folder or shortcut.
- Identify the options available within the Display Properties dialog box.

#### Unit 2: Windows NT Workstation Basics

Objectives:

- Use the different elements of the Windows NT Taskbar.
- Identify the purpose of items available on the Start Menu.
- Identify the order of the steps used to modify the Start Menu.
- Use the Start Menu to launch an application.
- Identify the functions of the Windows NT Workstation 4.0 Help utility.
- Identify ways that you can switch between open windows.
- Use options from the Desktop shortcut menu to arrange windows on the Desktop.

Unit 3: Using Explorer

Objectives:

- Identify the Explorer features to view files and folders.
- Identify the components of the Explorer window.
- Identify display options for files and folders in Explorer.
- Identify the features to change the view of files and folders in Explorer.
- Identify the steps to change the file association of an application using the shortcut menu.
- Preview a file using Quick View on the Shortcut menu.
- Create a new folder using the Explorer shortcut menu.
- Identify the selection method to select files and folders in Explorer.
- Complete the steps to copy/move a selection of files.
- Rename a file or folder using the shortcut menu.
- Create a shortcut to a folder using the shortcut menu in Explorer.
- Remove a file, folder or shortcut using the Explorer toolbar.
- Identify the steps used to format a diskette using the shortcut menu in Explorer.
- Identify the steps to copy a file to a diskette using the shortcut menu.
- Identify the best way to search for a particular file by specifying the name and location of the file.
- Identify the best way to search for a file modified on a certain date using the Find command on the Tools menu.
- Identify the advanced Find File features to use when searching for a file.
- Identify the best way to find a computer in a network environment.

## **Administering Microsoft Windows NT 4.0 - Part 1**

Course 71401

### **LEARN TO:**

- Identify the features of Windows NT 4.0 interface, create and customize user and group accounts.
- Administer rights and policies for user and group accounts and configure the user environment.
- Manage and secure resources with shared folders and NTFS permissions.

**COURSE LENGTH:** 6 - 8 hour(s)

### **Unit Names:**

Unit 1: Introduction to Microsoft Windows NT 4.0

Objectives:

- Identify the features of Windows NT Server Directory Services
- Log on to a domain.
- Match the various Administration Tools provided by Windows NT 4.0 with the tasks performed by each tool.
- Identify the functions of user accounts.
- Create a new user account.
- Copy an existing user account to make a new user account.
- Modify an existing user account by changing the password of the user account.
- Identify the features of the following groups: Local Groups; Global Groups; Default Groups; Special Groups
- Create a local group using the User Manager for Domains.
- Create a global group using the User Manager for Domains.

Unit 2: Managing User and Group Accounts

## NMCI Security Policy

### Objectives:

- Assign a user to a local group by creating an Administrator account. Enabler: Identify features of groups.
- Set an Account policy for all domain accounts. Enabler: Identify features of the Account policy.
- Set a User Rights policy for a user account. Enabler: Identify the features of user rights.
- Maintain Domain Controllers by: Synchronizing a given Backup Domain Controller(BDC) with the Primary Domain Controller(PDC). Promoting a given Backup Domain Controller(BDC) to function as a Primary Domain Controller(PDC).
- Match the common logon problems with their respective solutions.
- Identify the features of common user profiles: local profile, server based profile, user default profile, system default profile
- Identify the functions of a system policy.
- Set a new policy for all users using the System Policy Editor.

## Unit 3. Managing Resources

### Objectives:

- Share a folder with a limited number of users.
- Secure shared folders by assigning permissions to them.
- Add a new group to a list of groups that can access a shared folder.
- Identify the conditions under which a user is authorized to assign NTFS permissions.
- Assign NTFS permission in a single-domain network.
- Assign NTFS permission in a multiple-domain network.
- Identify the functions performed by the Disk Administrator to administer disk resources.
- Identify the methods to secure an Internet server.
- Take ownership of files and folders.
- Match the permission problems with their solutions.

## **Administering Microsoft Windows NT 4.0 - Part 2**

Course 71402

*Produced by NETg*

### **LEARN TO:**

- Create and administer network printers.
- Audit and monitor the server resources.
- Make backups and restore data from a tape.

**COURSE LENGTH:** 6 - 8 hour(s)

### **Unit Names:**

Unit 1: Creating and Administration of Network Printers

Objectives:

- Sequence the events in the Windows NT printing process.
- Create a network printer.
- Configure a network printer. Set the Spool Print Documents So Program Finishes Printing Faster option. Set the Hold Mismatched Documents option. Set the Print Spooled Jobs First option.
- Create a printer pool.
- Access a network printer.
- Assign the Full Control printer right to a user.
- Assign the Print printer right to a group.
- Assign Print Operator privileges to a user in a network.
- Assign Print Operator privileges to a user in a network.
- Pause a printer.
- Set the highest priority for a printer.
- Set the printing hours for a printer.



## NMCI Security Policy

- Purge a document from a print queue.
- Redirect a document sent for printing.
- Change the priority of a document so that it is printed before any other document in the print queue.
- Change the priority of a document so that it is printed before any other document in the print queue.
- Change the printer driver.
- Restart a stalled spooler in the Windows NT 4.0 setup.

## Unit 2: Auditing and Monitoring Server Resources

### Objectives:

- Set up an Audit policy for the Success and Failure of the Logon and Logoff event.
- Audit directories for Success and Failure of Read.
- Audit files for the Success and Failure of Write.
- Audit the printer for the Success and Failure of Print.
- Display the Audit Log using the Event Viewer.
- Set options for Audit Logs. Maximum Log Size. Overwrite Events Older than.
- Display a list of users connected to the server.
- Display a list of the shared resources of a server.
- Display the resources In Use using the Server Manager.
- Send administrative alerts to a user.
- Display configurations options using Windows NT Diagnostics(WinMSD).
- System option
- Memory option
- Use the Registry Editor to remotely administer a server from a client workstation.

## Unit 3: Backup and Restore Data

### Objectives:

- Identify the key factors for developing a system backup plan.
- Identify the functions of the Backup tool.
- Load a tape driver.
- Add a user to the Backup Operators group.
- Match the types of backups with their functions.

## NMCI Security Policy

- Send a message to all the users logged on to a server.
- Disconnect users before making a backup.
- Select files to be backed up using the Backup tool.
- Set tape options using the Backup tool. Verify After Backup Restrict Access To Owner Or Administrator.
- Set the backup set options using the Backup tool. Description Backup Type.
- Set the Full Detail Log Option.
- Schedule an automatic backup on a tape using the AT command.
- Identify the correct order in which the tapes are used to restore backups.
- Select the files to be restored from a tape.
- Restore files from a tape by setting the restore options. Restore to Drive Verify After Restore Restore File Permission Full Detail.
- Identify the function of Emergency Repair Disk.

## **UNIX Fundamentals**

Course 12327

*Produced by NETg*

### **LEARN TO:**

- Explain the origin, structure of UNIX and UNIX standards. Identify the different features and components of the

UNIX operating system.

- Identify the organization of data in the UNIX environment.

- Use UNIX editors to process text in UNIX files.

- Identify the types and functions of the various shells, and the shell variable settings to configure the UNIX

environment.

**COURSE LENGTH:** 6 - 8 hour(s)

### **Unit Names:**

Unit 1: Introduction to UNIX

Objectives:

- Identify the origins of the UNIX operating system:

- Place of development

- Founders involved

- Identify the features of the different versions of UNIX:

- SCO

- UNIX

- BSD

- XENIX
  - SVR4
  - AIX
  - SVID
  - LINUX
  - Identify the important features of the UNIX operating system:
    - Multiuser
    - Multitasking
    - Time Sharing
    - Portability
    - Networking
    - User Selectable Command Language
  - Identify the organizations that have defined the following UNIX standards:
    - POSIX
    - X/OPEN
    - OSF
    - XPG
  - Sequence the steps involved in the command interpretation done by the shell.
  - Identify the functions of the kernel.
  - Match the subdirectories of the root directory with their contents.
  - Match various utilities of UNIX with their functions:
- Log into the UNIX operating system.
- cal
  - lp
  - dc
  - grep
  - sccs
  - bc
  - make
- Log into the UNIX operating system.
  - Change the password associated with the login name using the passwd command.
  - Display online help for UNIX commands using the man command.

## NMCI Security Policy

- Log out of the UNIX system using the logout command.
- Identify the command to display the login information:
  - Current login name
  - Complete login information
- Exchange short messages on the UNIX operating system.
- Send mail to users using the mail command.
- Use the mail command to display messages.

## Unit 2: File and Directory Basics

### Objectives:

- Identify the definition of the following directories in UNIX:
  - the root directory
  - the home directory
  - the current directory
- Identify the definition of the types of files in UNIX:
  - ordinary files
  - directory files
  - special files
- Identify the correct file names used in UNIX.
- Match the metacharacters with their functions.
- Create a new directory using the mkdir command:
  - Create a new directory with mkdir using absolute pathname
  - Create a new directory with mkdir using relative pathname
- Display the current working directory using the pwd command.
- Change the working directory using the cd command.
- Display the list of files in a directory: List using ls command Long list using ls -l command.
- Remove a directory from the hard disk using the rmdir command.
- Create a new file using the cat command.
- Locate files using the -name and -print options of the find command.
- Copy files using the cp command.
- Move files from one directory to another using the mv command.
- Using the rm command to delete files:

- Delete a single file
- Delete multiple files together
- Control the file access permissions for various users using the chmod command:
  - Grant permissions
  - Revoke permissions.
- View the text of a file one page at time:
  - pg command
  - more command
- Search a string of text in a file using the look command.
- View a selective section of a file:
  - head command
  - tail command
- Arrange the contents of a file using the sort command.

### Unit 3: Text Processing in UNIX

#### Objectives:

- Identify the functions of the UNIX editor.
- Identify the features of the editors in UNIX:
  - line editor, ed
  - screen editor, vi.
- Create a file using the line editor ed.
- Type the command line to display a file opened in the ed editor.
- Edit text in a file using the ed editor.
- Exit from the ed editor.
- Create a file using the screen editor vi.
- Move to different locations in a file opened in the vi editor:
  - command mode
  - input mode
  - last line mode
- Edit a file using the vi editor:
  - Replace one character with another
  - Yank a paragraph
  - Remove a character
- Exit from the vi editor:

- while saving a file
- without saving a file

#### Unit 4: The UNIX Shell Environment

##### Objectives:

- Identify the command prompts of different types of shells:
  - C shell
  - Bourne shell
  - Korn shell
- Match the environment variables with their functions:
  - HOME
  - PATH
  - PS1
  - LOGNAME
  - TERM
- Display the values of variables:
  - Environment
  - Non-environment
- Set environment variables to specific values in different shells:
  - Bourne and Korn shells
  - C shell
- Remove a non-environment variable.
- Share variables among different shells.
- Identify the benefit for setting shell variables at system startup.
- Identify the startup files executed during the login sequence in shells:
  - Bourne and Korn shells
  - C shell
- Set shell variable in the .profile file:
  - Bourne shell
  - Korn shell
- Set shell variables in the C shell:
  - .cshrc file login file

- Control a process/job mechanism using the kill command.
- Give alias names to commands using the alias command in different shells: C shell Korn shell.
- Set the history mechanism in a shell:
  - C shell
  - Korn shell
- Manipulate a directory using the directory stack mechanism:
  - Put a directory in a stack
  - Pull a directory from a stack
- Use metacharacters to condense commands:
  - \*
  - []
  - #.
- Use the filename completion indicators to complete filenames at command line:
  - The ~(tilde) indicator
  - The [TAB] indicator



## **UNIX Intermediate Topics**

Course 12426

*Produced by NETg*

### **LEARN TO:**

- Identify the concept of standard input, standard output, standard error, and the methods of redirecting commands and control jobs.
- Identify the UNIX internal file representation, security methods for data access and the procedure to link files.
- Execute commands to manipulate ASCII and non-ASCII files.
- Use different UNIX commands to search, edit and print contents of a file.
- Understand the need for file processing utilities in UNIX including the usage of splitting, compressing, concatenating, disk spacing utilities.

**COURSE LENGTH:** 6 - 8 hour(s)

### **Unit Names:**

Unit 1: Input and Output Operations in UNIX

Objectives:

- Identify the definition of:
  - standard input
  - standard output
  - standard error
- Identify the different redirection operators.
  - Input redirection operator
  - Output redirection operator

## NMCI Security Policy

- Append redirection operator
- Redirect commands using redirection operators:
  - Using input redirection
  - Using output redirection
  - Using error redirection
- Set the noclobber variable to prevent overwriting existing files:
  - In Korn shell
  - In C shell
- Identify the definition of filters.
- Identify the use of a pipe.
- Redirect output of one command as input to another command.
- Store intermediate results of a pipe in a file using the tee command.
- Identify the benefits of controlling jobs.
- Control the execution of jobs:
  - Suspend a job
  - Resume a job
- Display the status list of jobs using the jobs command.
- Set the execution priority of a process using the nice command.
- Set the execution time of a command using the at command.

## Unit 2: Handling File Information

### Objectives:

- Match the sections of a file system with their respective functions: Boot Block Super Block inode List Data Block
- Identify the information stored in an inode.
- Identify the functions of an inode.
- Identify the benefits of using file links.
- Establish link between files using the ln command:
  - Establishing hard link
  - Establishing soft link
- Secure data in files using the crypt command:
  - Encrypt data using the crypt command
  - Decrypt data using the crypt command

- Lock the terminal using the lock command.

### Unit 3: File Operations in UNIX

#### Objectives:

- Compare two sorted files using the comm command.
  - Suppress display of data unique to the first file
  - Suppress display of data unique to second file:
  - Suppress display of data common to the two files
- Display a report of file comparison using the diff command.
- Compare two large files in segments using the bdiff command.
- Compare three files using the diff3 command:
  - Generate output in the form ed editor script
  - Incorporate all changes from file2 to file3 into file1
- Display the result of a simultaneous comparison of two files, using the sdiff command.
- Locate the first dissimilarity while comparing two files using the cmp command:
  - List the report in decimal byte number.
- Display the contents of a non-ASCII file using the cat -v command.
- Display the contents of a non-ASCII file in ASCII format using the od command.
- Compare three non-ASCII files using the -a option of the diff3 command.
- Identify the features of device special files in UNIX:
  - Character special files
  - Block special files
- Identify the need for having major and minor device numbers for a device special file.

### Unit 4: Manipulating and Printing File Contents

#### Objectives:

- Match the regular expression characters with their uses.
- Search for a pattern in a file using the grep command.
- Search for a fixed string pattern in a file using the fgrep command.
- Search extensively for a string containing regular expression characters using the egrep command.
- Compare adjacent lines in a text file using the uniq command:
  - Display only unique lines

- Display the duplicate lines
- Pull out the specific data fields from a text file using the cut command.
- Paste the lines of text files side by side using the paste command:
  - Use the default delimiter
  - Specify the delimiter being used
- Send a print request to a default printer using the -d option of the lp command.
- Print the contents of a file while simultaneously creating a copy of the file being printed.
- Display the print queue using the lpstat command.
- Cancel the request for printing a file using the cancel command.
- Create a typescript file using the script command:
  - Typescript created in a new file
  - Typescript appended to an existing file

## Unit 5: File Processing Utilities

### Objectives:

- Identify the need for file processing utilities in UNIX.
- Split a file into smaller files using the split command.
- Split a file based on context arguments using the csplit command.
- Identify the need for file compressing utilities.
- Pack a file using the pack command.
- Generate a report on the amount of disk space saved while compressing a file using the compress command.
- Uncompress a compressed file using the uncompress command.
- Display the combined output of the two packed files using the pcat command.
- Display the combined output of the two compressed files using the zcat command.
- Identify the need for the file space utilities.
- Generate a summary report on the usage of disk space by every file in a directory.
- Generate a report on the percent and number of free blocks available for file systems by using the df command.
- Display the size of a file in blocks using the ls -ls command.
- Execute a command a specified number of times using the xargs command.

## **TCP/IP - Concepts and Architecture**

Course 12258

*Produced by NETg*

### **LEARN TO:**

- Describe TCP/IP in terms of a standard protocol for internetworking, its evolution, services provided and its architecture.
- Describe the system of addressing and routing in TCP/IP.
- Describe the key features and services of two transport protocols of TCP/IP, TCP and UDP.
- Describe the protocols that support the services in the TCP/IP Application layer.

**COURSE LENGTH:** 6 - 8 hour(s)

### **Unit Names:**

Unit 1 -- TCP/IP Overview

Objectives:

- Identify the definition of TCP/IP.
- Identify the reasons why TCP/IP was developed.
- Sequence the events that took place in the evolution of TCP/IP.
- Define the role of various bodies in setting standards for TCP/IP.
- Identify the functions of the application level services provided by TCP/IP:
  - Electronic mail.
- File transfer.
- Remote login.
- Identify the functions of the network level services provided by TCP/IP:
- Connection-oriented service.

- Connection-less packet delivery service.
- Identify the unique features of services provided by TCP/IP.
- Identify the need to have multiple layers of protocol.
- Identify the functions of each layer of ISO model.
- Identify the functions of each layer of TCP/IP protocol suite.
- Define common network terms and components:
  - Host
  - Host address
  - Physical network
  - Physical network address
  - IP address
  - IP datagram
  - Ports
  - Segment
  - IP Router
  - Router
  - Routing Table
- Sequence the steps involved in data flow between adjacent nodes.
- Sequence the steps involved in data flow between non-adjacent nodes.

## Unit 2 -- TCP/IP Internet layer: Addressing and Routing

### Objectives:

- Identify the range of different classes of IP address.
- Identify the definition of Dotted Decimal Notation.
- Identify the uses of IP address.
- Identify the methods of resolving TCP/IP Addresses.
- Sequence the steps in resolution of addresses using ARP.
- Sequence the steps involved in the using RARP.
- Identify the key features of Internet Protocol (IP).
- Identify the function of the components of IP Datagram.

## NMCI Security Policy

- Sequence the steps in fragmentation and reassembly of IP datagram.
- Identify the definition of ICMP.
- Identify the information stored in Routing Tables.
- Identify the key features of Vector Distance routing.
- Identify the key features of GGP.
- Identify the key features of EGP.
- Identify the key features of the following IGP Protocols:
  - RIP
  - OSPF
  - Hello

## Unit 3 -- Transport Layer

### Objectives:

- Identify the need for TCP.
- Identify the definition of key features of TCP.
- Identify the key services provided by TCP:
  - Multiplexing
  - Connection Management
  - Data transfer
  - Urgent Data Signaling
  - Data Stream Push
  - Error Reporting
- Identify the functions of the components of TCP/IP header.
- Sequence the steps in establishing a TCP .  
connection.
- Sequence the steps in closing the connection in normal and abnormal situations.
- Match the factors influencing TCP performance with the causes that give rise to them.
- Identify the key features of UDP.
- Identify the contents of a UDP header.
- Sequence of steps used in UDP dataflow.

## Unit 4 -- TCP/IP Application Layer Protocols

Objectives:

- Identify the key features of FTP.
- Sequence the steps involved in transfer of files from a remote computer using FTP.
- Identify the key features of NFS.
- Sequence the steps in accessing remote files using NFS.
- Identify the definition of the following key terms used in E-mail:
  - E-mail address
  - E-mail message
  - E-mail alias
  - Electronic mailing list
- Sequence the steps in E-mail delivery.
- Identify the role of SMTP in E-mail delivery.
- Identify the functions of DNS.
- Sequence the steps in resolution of Domain names.
- Identify the definition of TELNET.
- Identify the services provided by TELNET.
- Identify the definition of SNMP.
- Identify the management services offered by SNMP.
- Identify the functions of Kerberos.
- Identify the key features of Kerberos.



LEVEL II

**System Administrator Level 2 Certification Criteria**

**System Administrator Level 2 Certification requires the following technical training, IA training, and on-the-job experience:**

- **Level 1 certification**
- and**
- **Formal technical training equivalent to Level 2 Technical Training Minimum Standards<sup>1</sup>**
- and**
- **Formal IA training equivalent to Level 2 Information Assurance Training Minimum Standards<sup>2</sup>**
- and**
- **3 years System Administrator experience**

**Notes**

**<sup>1</sup> Level 2 Technical Training Minimum Standards**

**Formal technical training in the following areas:**

- **heterogeneous networks**
- **network devices and troubleshooting**
- **basic installation, configuration, troubleshooting, and management of Windows NT system in a network environment**
- **installation and configuration of DHCP, WINS, LM Host, IIS**
- **implementation of Windows NT Directory Services**
- **basic installation, configuration, administration, and troubleshooting of Microsoft Exchange Server 5.5**
- *Asynchronous Transfer Mode, Wide Area Networks, T-1 circuits, Packet Switched Networks, and Integrated Services Digital Networks*
- **basic installation, configuration, troubleshooting, and management of UNIX server environments**

- **basic UNIX shell programming**

### **Equivalent CNET Schools**

*CNET Information Systems Administrator (ISA) Course (NEC 2735)*

*CNET Cryptologic Network and Systems Configuration Manager Course (NEC 9302)*

Equivalent NETg Technical Training COI for Level 2

<b><u>Course #</u></b>	<b><u>Course Title</u></b>
71443	MS Networking Essentials 2nd ed. - Part 3
71444	MS Networking Essentials 2nd ed. - Part 4
71410	MS Windows NT 4.0 Core Technologies - Part 1
71411	MS Windows NT 4.0 Core Technologies - Part 2
71412	MS Windows NT 4.0 Core Technologies - Part 3
71413	MS Windows NT 4.0 Core Technologies - Part 4
71414	MS Windows NT 4.0 Server Implementing Directory Services
73361	Microsoft Exchange Server 5.5 Concepts and Administration - Part 1
73362	Microsoft Exchange Server 5.5 Concepts and Administration - Part 2
73363	Microsoft Exchange Server 5.5 Concepts and Administration - Part 3
12756	Networking Technology Series: ATM
12672	UNIX Advanced Topics
12777	UNIX Shell Programming
6.0	12778 UNIX SVR4 System Administration Fundamentals

*Total of 14 classes, approximately 100 hours of training.*

## <sup>2</sup> **Level 2 Information Assurance Training Minimum Standards**

**Formal IA training in the following areas:**

- identification of security threats
- identification of tools for protecting networks
- methods of implementing LAN security
- strategies for protecting system security
- firewall and proxy server management
- intrusion detection
- security issues and solutions in Web Site management
- gaining Internet access and securing the gateway
- creating a secure Internet messaging channel

## NMCI Security Policy

- addressing security risks associated with Java, CGI and viruses

### Equivalent CNET Schools

CNET Network Security Vulnerability Technician (NSVT) Course (NEC 2780)

### Equivalent NETg IA COI for Level 2

<u>Course #</u>	<u>Course Title</u>
12764	Network Security
12700	Web Site Security - Part 1
12703	Web Servers Implementing and Administering - Part 1

**Networking Essentials 2nd Edition - Part 3**

Course 71443

*Produced by NETg*

**LEARN TO:**

- Identify the functions of the network operating system and its components.
- Install and configure a network operating system.
- Identify the characteristics and advantages of the client/server model and its components
- Manage network accounts and data security.
- Monitor network performance.

**COURSE LENGTH:** 6 - 8 hour(s)

**Unit Names:**

Unit 1: Network Operations

Objectives:

- Identify the functions of the network operating system.
- Identify the characteristics of the two types of multitasking:

Preemptive

Cooperative.

- Identify the role of the redirector in the functioning of the network operating system.
- Identify the role of the server software in a network operating system.
- Identify the prerequisite for the installation of the Windows NT 4.0 network operating system.
- Install the file system on a computer during the installation of Windows NT server 4.0.
- Set the server parameters while installing Windows NT server 4.0 on a computer.
- Configure the network environment for Windows NT server 4.0 being installed on a computer.
- Configure the server environment while installing Windows NT server 4.0 on a computer.

- Install a network service from the Control Panel.
- Sequence the steps that are involved in resolving NetBIOS names by using Microsoft methods.
- Set up a shared printer in the Microsoft Windows NT 4.0 environment.
- Connect to a shared printer in the Microsoft Windows NT 4.0 network.
- Identify the tasks involved in managing a shared printer.
- Identify the tasks that are enabled by the shared fax modem.
- Identify the features of e-mail.
- Match the e-mail standards with the services they provide.
- Identify the functions of scheduling.
- Identify the task for which groupware is used.
- Match the groupware programs with their features:

Groupware e-mail

Groupware multimedia

Microsoft Windows 95

Banyan Intelligent Messaging Service

TeamLinks

Novell GroupWise

- Identify the features of the groupware products:

Microsoft Exchange

Lotus Notes

- Set up a shared application on the Windows NT server 4.0 network.
- Match the appropriate vendor option for interoperability with a given situation.
- Identify the characteristics of the client/server model and centralized computing.
- Identify the functions of the client in the client/server model.
- Identify the functions of the server in the client/server model.

## Unit 2: Network Administration and Support

### Objectives:

- Identify the responsibilities of a network administrator.
- Create a user account for a given username by using the User Manager for Domains.
- Match the different group accounts with their characteristics.
- Create a local group by using the User Manager for Domains.

- Delete a user account by using the User Manager for Domains.
- Given a situation, identify the best measures to manage the user accounts.
- Identify the situations that cause network device bottlenecks.
- Match the network performance monitoring tools with their functions:

Windows NT Performance Monitor

Windows NT Network Monitor

Simple Network Management Protocol (SNMP)

- Identify the functions of Microsoft Systems Management Server (SMS) used for system management.
- Select the appropriate administrative plan to meet the given network performance management requirements.
- Identify the strategies that help in developing a preemptive network security plan.
- Set up a shared folder on the network with share level security.
- Set up a shared folder on the network with user level security.
- Match the security enhancement methods with their features.
- Select the security plan best suited to the given network security requirements.
- Identify the guidelines for implementing a backup system.
- Identify the functions of a UPS system.
- Match the different fault tolerance systems with the given requirements.

**Networking Essentials 2nd Edition - Part 4**

Course 71444

*Produced by NETg*

**LEARN TO:**

- Examine the devices and technologies that are used to expand a network across the street or around the world.
- Identify the basic concepts and approaches involved in maintaining a network.

**COURSE LENGTH:** 6 - 8 hour(s)

**Unit Names:**

Unit 1: Larger Networks

Objectives:

- Identify the factors that affect the performance of modems.
- Identify the specifications that would be best fulfilled by a type of modem.
- Identify the specifications that would be best fulfilled by a type of carrier.
- Identify the features of the remote access capability provided with the help of RAS and PPTP.
- Identify the ways in which LAN expansion components increase the size of a network.
- Identify the functions of repeaters.
- Identify the functions of bridges.
- Identify the functions of routers.
- Identify the functions of brouters.
- Identify the function of gateways.
- Match each LAN expansion component with the situation for which it is best suited.
- Identify the transmission technologies used in WANs.
- Identify the specifications that would be best fulfilled by a type of analog connectivity.
- Match the digital lines with their features.



- Identify the features of packet-switching networks.
- Match the key advanced WAN technologies with their descriptions.
- Identify the features of the X.25 packet-switching technology.
- Identify the features of the Frame Relay technology.
- Identify the features of the ISDN technology.
- Identify the cell relay technology that is suitable in a given situation.
- Identify the fiber-optic technology that is suitable in a given situation.
- Match each WAN technology with the situation for which it is best suited.

## Unit 2: Solving Network Problems

### Objectives:

- Identify the strategies that help to incorporate a preemptive troubleshooting approach into a network plan.
- Identify the network monitoring functions performed by Performance Monitor.
- Sequence the steps that constitute a structured troubleshooting approach.
- Identify the troubleshooting tools to be used in a given situation.
- Identify the types of network behavior information provided by protocol analyzers.
- Match the network support resources with their advantages.
- Match the common network problems with the troubleshooting approaches.
- Match the Internet services with their uses.
- Identify the characteristics of Microsoft Network.
- Sequence the components of an URL.
- Identify the type of Internet connection that is suitable in a given situation.

**Supporting Microsoft Windows NT 4.0 Core Technologies - Part 1**

Course 71410

*Produced by NETg*

**LEARN TO:**

- Describe the Windows NT environment, its architecture and the network models.
- Install the Windows NT Server 4.0 as a Primary Domain Controller in a Single Domain Model.
- Configure the Windows NT environment using the Control Panel, Registry Editor and the System Policy Editor.
- Distinguish between User Profiles and System Policies, create user profiles and manage System Policies using the System Policy Editor.

**COURSE LENGTH:** 6 - 8 hour(s)

**Unit Names:**

Unit 1: Introduction to Microsoft Windows NT

Objectives:

- Identify the features of Windows NT and the Microsoft operating system family.
- Identify the features of the operating systems in the Microsoft operating system family.
- Windows 95.
- Windows NT Server.
- Windows NT Workstation.
- Identify the functions of the security features of Windows NT.
- Mandatory logon.
- Access token.
- Account lockout.
- Identify the functions of the subsystems running in the User Mode.
- POSIX subsystem.

## NMCI Security Policy

- OS/2 subsystem.
- WIN32 subsystem.
- Match the Executive Services components with their functions.
- HAL.
- Microkernel.
- Process Manager.
- Object Manager.
- Virtual Memory Manager.
- Local Procedure Call Facility.
- Security Reference Monitor.
- I/O Manager.
- Identify the features of the Windows NT memory model.
- Identify the features of the Workgroup model and the Domain model.
- Sequence the steps of Windows NT logon process.
- Logging on to a Windows NT-based computer.
- Logging on to a domain.

## Unit 2: Installing the Windows NT Server

### Objectives:

- Identify the system requirements for installing the Windows NT Server 4.0.
- Hardware requirements.
- Network adapter.
- Network protocols.
- Determine the domain requirements to install the Windows NT Server 4.0.
- Identify the features of the installation Setup options.
- Typical Setup option.
- Portable Setup option.
- Compact Setup option.
- Custom Setup option.
- Install the FAT file system for the Windows NT Server 4.0.
- Configure the Windows NT Server 4.0 as a Primary Domain Controller.
- Specify computer name.

## NMCI Security Policy

- Specify role of the server as a PDC.
- Specify administrator account.
- Configure the Windows NT Server network environment.
- Specify Network Adapter Card.
- Specify Network Protocols.
- Specify IRQ level.
- Specify I/O Port Address.
- Set the Windows NT Server environment parameters.
- Specify computer name.
- Specify domain name.
- Specify time zone and system date.
- Identify the appropriate action that will resolve the installation failure.
- Identify the components that are preserved during the upgrade process of Windows NT 3.x to 4.0.
- View the help file from the Windows NT Server Books Online.
- Sequence the steps to uninstall the Windows NT 4.0.
- Uninstall from a FAT partition.
- Uninstall from an NTFS partition.

## Unit 3: Configuring Windows NT Environment

### Objectives:

- Identify the functions and the structure of the Registry.
- Identify the uses of the Windows NT Registry.
- Match the Registry subtrees with their contents.
- HKEY\_LOCAL\_MACHINE.
- HKEY\_CURRENT\_USER.
- HKEY\_USERS.
- HKEY\_CLASSES\_ROOT.
- HKEY\_CURRENT\_CONFIG.
- Identify the features of hives.
- Configure system hardware and software using the Control Panel.
- Configure the mouse driver using the Control Panel.
- Configure the Display settings using the Control Panel.

## NMCI Security Policy

- Install device drivers for SCSI adapters.
- Configure a modem.
- Modem type.
- Port.
- Area code.
- Dialing type.
- Change the size of the Paging file using the Control Panel.
- Identify the sequence in which Windows NT sets environment variables.
- Access the Registry information using the Registry Editor.
- Change Registry settings using the System Policy Editor.
- Create a logon banner.
- Disable the display of the last logged-on user name.

## Unit 4: User Profiles and System Policies

### Objectives:

- Identify the advantages of user profiles.
- Identify the features of the different types of user profiles.
- Manage Roaming User Profiles.
- Create a Roaming profile for a user.
- Copy profile information to a server.
- Identify the functions of a system policy.
- Set a new policy for all users using the Policy Editor.
- Identify the template files used to create policies.
- Windows NT computers.
- Windows 95 computers.

**Supporting Microsoft Windows NT 4.0 Core Technologies - Part 2**

Course 71411

*Produced by NETg*

**LEARN TO:**

- Describe the Windows NT file systems, manage partitions and configure the hard disk.
- Manage disk resources by creating and securing the resources.
- Protect Server data using various Windows NT fault tolerance levels, Data Protection and Data Recovery methods.

**COURSE LENGTH:** 6 - 7 hour(s)

**Unit Names:**

Unit 1: Managing File Systems

Objectives:

- Identify the features of the two primary file systems supported by Windows NT.
- FAT
- NTFS
- Identify the autogenerated short filename, given a Windows NT long filename.
- Given a folder, manage NTFS compression.
- Compress a folder including subfolders.
- Uncompress a folder including subfolders.
- Create partitions using the Disk Administrator.
- Create a primary partition.
- Create a logical drive on an extended partition.
- Format the partition with a file system, given the Disk Administrator window.
- NTFS
- FAT

## NMCI Security Policy

- Convert a FAT partition to NTFS using the convert command.
- Identify the features of an active partition.
- Manage volume sets, given the Disk Administrator window.
- Create a volume set.
- Extend a volume set.
- Delete a volume set, given the Disk Administrator window.
- Manage a stripe set, given the Disk Administrator window.
- Create a stripe set.
- Delete a stripe set.

## Unit 2: Managing Disk Resources

### Objectives:

- Create a folder and make it shareable.
- Assign shared folder permissions.
- Assign the NTFS permissions for the shared folder to specific groups.
- Match the copy and move tasks with the changes in the permissions set on a file.
- Within an NTFS volume.
- Between NTFS volumes.
- From NTFS to FAT volumes.
- From FAT to NTFS.
- Given the Windows NT Explorer window, take ownership of files and folders.
- Audit the user account database.
- Establish file auditing for a specific operation, given the Windows NT Explorer window.

## Unit 3: Fault Tolerance RAID Levels

### Objectives:

- Match the Redundant Arrays of Inexpensive Disks (RAID) levels with their features.
- Given a situation, select the best suited fault tolerance method.
- Create a mirror set using the Disk Administrator.
- Create a stripe set with parity using the Disk Administrator.
- Implement the appropriate data recovery method on a Windows NT fault tolerant system.
- Sequence the steps to recover a broken mirror set.

## NMCI Security Policy

- Regenerate a stripe set with parity to recover data.



## **Supporting Microsoft Windows NT 4.0 Core Technologies - Part 3**

Course 71412

*Produced by NETg*

### **LEARN TO:**

- Identify the subsystems responsible for supporting applications.
- Manage the applications with Task Manager and the Command Prompt.
- Identify the common application-related problems in Windows NT.
- Identify the Windows NT components that provide networking capabilities.
- Describe the evolution of the Internet and the Intranet.
- Identify the features of the network protocol.
- Install and configure the TCP/IP, NWLink and NetBEUI protocols.
- Identify the default network components and configure the bindings.
- Identify the features of Browser Service.
- Install and configure DHCP, WINS and DNS.
- Access resources in a remote network.

**COURSE LENGTH:** 6 - 8 hour(s)

### **Unit Names:**

Unit 1: Applications Supported by the Windows NT Server

Objectives:

- Identify and configure the components required to support different types of applications.
- Identify the features of the Win32-based applications supported by Windows NT.
- Sequence the steps of the Win16 on Win32 (WOW) operation to run a WIn16-based application.
- Identify the features of POSIX subsystem supported by Windows NT Server.
- Identify the features of OS/2-based application-support by Windows NT:

Intel x86-based computers.

RISC-based computers.

## NMCI Security Policy

- Identify the common application-related problems in Windows NT.
- Identify the uses of the Command Prompt.
- Use the Task Manager:

Close an application using the Task Manager.

Set a priority level for an application using the Task Manager.

## Unit 2: Windows NT-Based Networking Environment

### Objectives:

- Identify the Windows NT 4.0 networking components.
- Identify the functions of the boundary layers in the I/O Manager:

Network Device Interface Specification (NDIS) 4.0.

Transport Driver Interface (TDI).

- Identify the technology components of the Internet and the advantages of the Intranet.

## Unit 3: Network Protocols Configuration

### Objectives:

- Identify the features of the Transmission Control Protocol/Internet Protocol (TCP/IP).
- Install the Transmission Control Protocol/Internet Protocol.
- Configure the IP Address, Subnet Mask, and Default Gateway parameters of the TCP/IP.
- Install the NWLink transport protocol on the Windows NT Server.
- Configure the frame type and internal network number of the NWLink IPX/SPX protocol.
- Install the NetBIOS extended user interface (NetBEUI) protocol.
- Configure the network bindings.

## Unit 4: Windows NT Networking Services

### Objectives:

- Identify the features of Browser Service and the sequence of steps in a browser service.
- Identify the advantages of using Dynamic Host Configuration Protocol (DHCP) to configure an IP Address.
- Install the DHCP service on the Windows NT Server.
- Configure a DHCP scope on the Windows NT Server.
- Configure TCP/IP to automatically use DHCP.
- Install Windows Internet Name service (WINS) on the Windows NT Server.

## NMCI Security Policy

- Install the Domain Name Service (DNS) on the Windows NT Server.
- Configure the DNS service.

### Unit 5: Remote Access Service

#### Objectives:

- Install Remote Access Service (RAS) through the Network program item of the Control Panel.
- Install the Remote Access Service (RAS) software.
- Configure RAS with the TCP/IP Protocol.
- Configure the RAS server to support the NetBEUI protocol.
- Configure RAS with the IPX protocol.
- Create the DEVICE.LOG file to aid troubleshooting a modem problem.
- Create the PPP.LOG file to aid troubleshooting PPP authentication problems.
- Identify the features of TAPI and configure a TAPI location.
- Configure RAS Permissions to ensure the validity of the user accessing the RAS server:

Grant dial-in permissions.

Revoke dial-in permissions.

- Configure the RAS server for callback security options using the Remote Access Admin tool:

Preset To.

Set By Caller.

No Callback.

- Configure encryption to ensure RAS security:

Data encryption.

Password encryption.

## **Supporting Microsoft Windows NT 4.0 Core Technologies - Part 4**

Course 71413

*Produced by NETg*

### **LEARN TO:**

- Identify the benefits of integrating Intranet with the Internet.
- Identify the methods for assigning an IP address on the Intranet server.
- Install and configure Internet Information Server and the Microsoft Internet Explorer.
- Identify the Windows NT tools for NetWare.
- Install and configure the Gateway Services for NetWare.
- Use the Migration Tool to migrate user information from a NetWare server to a Windows NT Server and configure the user options in the Migration Tool.
- Identify the steps in the Windows NT printing process, configure network printers, use different print utilities and troubleshoot common printing problems.
- Identify licensing options, add Client Access Licenses in different modes and configure licensing replication.
- Identify tools to administer NT Servers from various clients and configure Windows NT for client computers.
- Replicate directories using the Directory Replicator service and synchronize files using the My Briefcase utility.
- Monitor system performance using the Performance Monitor and use the various Windows NT utilities to monitor system information.
- Identify bottlenecks and troubleshoot various system errors.

**COURSE LENGTH:** 6 - 8 hour(s)

### **Unit Names:**

Unit 1: Internet and Intranet Services

Objectives:

- Identify the benefits of integrating Intranet with the Internet.
- Identify the functions of the Internet Information Server.
- Given a Windows NT server with TCP/IP, install the Internet Information server.
- Given that IIS has been installed successfully, configure the Internet Information server.
- Identify the requirements for the installation of the Peer Web Services (PWS).
- Install the Microsoft Internet Explorer on a Windows NT server.
- Configure the Microsoft Internet Explorer.
- Reduce the number of viewed pages.
- Change the background color of the Explorer window.

Unit 2: Windows NT Interpretability with NetWare

Objectives:

- Match the Windows NT tools for NetWare with their functions.
- Client Services for NetWare (CSNW).
- Gateway Services for NetWare (GSNW).
- File and Print Services for NetWare (FPNW).
- Directory Service Manager for NetWare (DSMN).
- Identify the uses of Gateway Services for NetWare (GSNW) and the requirements for installing GSNW.
- Configure Gateway Services for NetWare.
- Match the GSNW problems with their respective troubleshooting solutions.
- Startup problems.
- Access problems.
- Application and print problems.
- Other network problems.
- Identify the advantages of the Migration Tool for NetWare.
- Identify the requirements for using the Migration Tool.
- Configure the Migration Tool.

Unit 3: Windows NT Printers

Objectives:

- Add and configure remote, local and NetWare based printers on Windows NT Server 4.0.

## NMCI Security Policy

- Identify the Windows NT printing components.
- Printer driver.
- Spooler.
- Print processor.
- Print monitor.
- Add a network printer.
- Configure a printer on a Windows NT server.
- Take the appropriate steps to correct common printing problems.
- Add the correct printer driver to the printer.
- Enable the spooling option on the printer.
- Identify the features of a printer pool.
- Set up print priorities.

## Unit 4: Network Clients

### Objectives:

- Identify the situations in which different Client Licensing options are used.
- Add Client Access Licenses to a Windows NT Server in the correct licensing mode.
- Configure licensing replication on a Windows NT Server.
- Given a Windows NT workstation, configure it as a client computer to Windows NT Server.
- Identify the advantages of Services for Macintosh.
- Identify the functions of the server tools used to administer Windows NT Server from Windows NT Workstations.

## Unit 5: Data Synchronization and Replication

### Objectives:

- Identify the purpose of directory replication.
- Identify the directory replication process and components.
- Configure the Directory Replicator service to log on as the special user for this account.
- Replicate files from the export server to the import computer.
- Identify the features of full file synchronization.
- Synchronize files using the My Briefcase utility.

## Unit 6: Troubleshooting Windows NT Server 4.0

Objectives:

- Use the Performance Monitor to monitor the activity of the processor.
- Use the Performance Monitor to monitor memory usage in the system.
- Use the Performance Monitor to monitor the Paging File object.
- Use the Performance Monitor to monitor the disk activity on the server.
- Identify the features of the counters used for monitoring the overall network activity.
- Pool Nonpaged Failures.
- Pool Nonpaged Peak.
- Bytes Total/sec.
- Frames Bytes Received/sec.
- Frames Received/sec.
- Frames Rejected/sec.
- Times Exhausted.
- Identify the threshold values of the counters in the Performance Monitor.
- Use the Event Viewer to view event logs.
- View the event logs.
- View the event logs of other computers.
- View the logs according to type.
- Use the Windows NT Diagnostics (WinMSD) utility to view system details.
- Services.
- Resources.
- Network.
- Install the Network Monitor.
- Resolve common boot failures using the Windows NT utilities.
- Update the system information using the Emergency Repair Disk.
- Resolve configuration errors by editing the Interval parameter in the Registry.
- Backup the Registry.
- Restore the Registry from the tape backup.
- Install and use Microsoft TechNet.

## **Implementing Directory Services in Microsoft Windows NT Server 4.0**

Course 71414

*Produced by NETg*

### **LEARN TO:**

- Implement Directory Services using Windows NT Server 4.0.
- Establish and manage trust relationships between domains.
- Select the most suitable Directory Services structure for a given business situation.
- Identify the issues involved in planning an effective Directory Services structure for an organization running

Windows NT Server 4.0.

**COURSE LENGTH:** 6 - 8 hour(s)

### **Unit Names:**

Unit 1: Implementing Windows NT Directory Services

Objectives:

- Identify the advantages of Windows NT Directory Services.
- Identify the functions of different Windows NT components which provide enterprise-wide communication:

Domains

Trusts

- Identify the functions of a single user account.
- Sequence the steps involved in the process of accessing a resource from any domain.
- Identify the functions of the utilities used by a network administrator to manage any account on the network:

User Manager

Server Manager

- Identify the advantages of the tools used by a network administrator to ensure smooth network



operation automatically:

Database Synchronization

Database Partitioning

- Identify the functions of DSMN.
- Identify the functions of BackOffice applications.

## Unit 2: Establishing Trust Relationships

Objectives:

- Identify the features of the types of trust relationships:

One-way trust relationship

Two-way trust relationship

- Identify the function of different types of domains:

Trusted domains

Trusting domains

- Identify the guidelines for implementing trust relationships.
- Identify the functions of accounts in trust relationships:

Local accounts

Global accounts

- Identify the guidelines for establishing group strategies across trusts.
- Assign the required access rights for users in a given local group.
- Identify the functions of the NetLogon service.
- Sequence the steps involved in the trusted domain logon process.
- Identify the requirements for establishing a trust between two domains.
- Implement a one-way Trust Relationship between two given domains.
- Implement a two-way Trust Relationship between two given domains.
- Identify the problems that can complicate trust functions.

## Unit 3: Selecting a Directory Services Structure

Objectives:

- Match the domain models in Windows NT Directory Services with their features:

Single domain model

Single master domain model

Multiple master domain model

Complete trust domain model

- Identify the factors that influence planning of a Directory Services domain structure.
- Identify the means through which a client computer can interact with a domain:

Windows NT-based computer

Non-Windows NT computer

- Identify the situation best suited for the single domain model.
- Identify the situation best suited for the master domain model.
- Identify the situation best suited for the multiple master domain model.
- Identify the situation best suited for the complete trust domain model.
- Identify the features of groups in a single master domain model:

Local groups

Global groups

- Sequence the steps involved in providing a user access to resources in another domain in a multiple master domain environment.
- Sequence the steps involved in implementing groups to perform backups in a master domain model.

#### Unit 4: Planning Directory Services Structure

Objectives:

- Identify the guidelines for achieving efficient network operations in Windows NT Directory Services.
- Identify the space considerations for managing accounts within the Directory Services database.
- Identify the recommended minimum hardware configuration for a domain controller, given the SAM file size and the number of user accounts.
- Identify the factors influencing the optimum number of master domains within a network.
- Identify the minimum number of backup domain controllers required to provide logon validation to a given number of user accounts in master domains.
- Identify the features of resource domains in a Windows NT Directory Services environment.
- Identify the factors influencing the determination of optimal server locations on the network.
- Identify the considerations that should be kept in mind while planning physical locations of BDCs across WAN links.
- Identify the effect of different Registry value entries on synchronization of account database replication:

ChangeLogSize

PulseConcurrency

- Identify the factors influencing the estimation of monthly replication time for a domain.
- Identify the ways to improve the performance of replication process over a slow WAN link.

**Microsoft Exchange Server 5.5 Concepts and Administration - Part 1**

Course 73361

*Produced by NETg*

**LEARN TO:**

- Identify the different types of messaging systems and understand the fundamentals of Exchange Server.
- Administer the Exchange Server by understanding the communication between the various components of Exchange Server, the Administrator Program and the Windows NT Tools.
- Work with the recipients in Microsoft Exchange Server 5.5.

**COURSE LENGTH:** 6 - 8 hour(s)

**Unit Names:**

Unit 1: Exchange Server: Introduction

Objectives:

- Identify the features of shared-file messaging systems.
- Identify the features of the client/server messaging systems.
- Identify the means by which Exchange Server is compatible with other messaging and operating systems.
- Match the various administrative units in an Exchange Server hierarchy with their features.
- Identify the Windows NT security features that have been integrated with Exchange Server.
- Match the core components of Exchange Server messaging infrastructure with their functions.
- Match the additional components of Exchange Server messaging infrastructure with their functions.
- Identify the features of the Microsoft Outlook client.
- Identify the new features of Exchange Server 5.5.

## Unit 2: Exchange Server Administration

### Objectives:

- Identify the purpose of the communication initiated by the core components.
- Identify the purpose of the communication initiated by the Administrator Program.
- Identify the purpose of the communication between the Exchange Server clients and core components.
- Identify the purpose of the communication initiated by the additional components.
- Sequence the steps for a single-server message flow between clients.
- Identify the functions of the Administrator Program.
- Match the objects in the Exchange Server Organizational hierarchy represented in the Administrator Program window with their functions.
- Match the Administrator Program command line switches with their functions.
- Match the different roles in an Exchange Server with their permissions.
- Match the customization options supported by the Administrator Program with their functions.
- Match the Windows NT Server Administration Tools with their functions.
- Create a mailbox by using User Manager for Domains extension (Mailumx.dll).

## Unit 3: Working with Recipients

### Objectives:

- Match the recipient object types with their functions.
- Match the common recipient object tabs with their functions.
- Create a recipient container by using the menu bar of the Microsoft Exchange Administrator Window.
- Create a mailbox by using the Windows NT User Manager.
- Create a mailbox for an existing Windows NT account by using the Microsoft Exchange Administrator.
- Configure a mailbox by using the mailbox configuration property pages.
- Create a custom recipient by using the toolbar of Microsoft Exchange Administrator.
- Configure a custom recipient by changing the e-mail address information by using the property sheet of the recipient.
- Create a distribution list by using the toolbar of the Microsoft Exchange window.
- Configure a distribution list by designating an expansion server.
- Configure the Exchange Server permissions by granting a global group, the role of Permissions

Admin on a Site object.

- Export directory information for a recipient.
- Import the directory information for a recipient.
- Duplicate and locate a recipient.
- Move a mailbox to another server within a site.
- Clean a mailbox by deleting messages.
- Group recipient objects by creating Address Book views.

## **Microsoft Exchange Server 5.5 Concepts and Administration - Part 2**

Course 73362

*Produced by NETg*

### **LEARN TO:**

- Describe client installation requirements and select the installation method to be used for installing an Outlook client.
- Describe the optional tabs in Microsoft Outlook and the configuration of offline and remote connection.
- Configure the order of protocols that RPCs use and use Windows NT system policies to manage an Outlook configuration.
- Configure SMTP addresses, custom attributes, search dialog objects and search permissions.

**COURSE LENGTH:** 6 - 8 hour(s)

### **Unit Names:**

Unit 1: Deploying Exchange Server Clients

Objectives:

- Identify the tasks that can be performed by using Outlook.
- Identify the tasks that can be performed by using Outlook for Windows 3.x.
- Identify the tasks that can be performed by using Outlook for Macintosh.
- Identify the tasks that can be performed by using Outlook Express.
- Identify the tasks that can be performed by using Outlook Web Access.
- Match the different Exchange clients with their installation.
- Select the appropriate installation method to be used for installing an Outlook client.
- Identify the functions of an Outlook client profile.

- Identify the process by which an Outlook client profile is created.
- Sequence the steps that occur when the Profgen utility is used to automatically create a client profile.
- Specify the name of the Exchange server in the Default.Prfl file.
- Specify the name of the logon script in the Windows NT account.
- Create a Personal Folder Store.
- Match the information services available to an Outlook client with their uses.
- Match the Exchange server clients with their method of connecting roving users to the Exchange server.

## Unit 2: Configuring and Managing Outlook

### Objectives:

- Match the tabs in the Options dialog box of Microsoft Outlook with the tasks that they enable.
- Configure the tabs in the Options dialog box of Microsoft Outlook for a specific situation.
- Grant the Send-On-Behalf-Of delegate access to a user.
- Grant the Send-As delegate access to a user.
- Import existing information from other programs into an Microsoft Outlook client by using the Import and Export Wizard.
- Configure Microsoft Outlook to use an offline folder.
- Synchronize all offline folders while working online.
- Sequence the steps to download mail headers from a Microsoft Exchange server to a remote client.
- Match the various RPC methods with the mechanisms they use for communicating with an Microsoft Exchange server.
- Configure the order of protocols RPCs use to connect from a Windows NT or 95 client to an Microsoft Exchange server.
- Identify the tasks that can be performed by using the System Policy Editor.
- Add a system policy template file to an Exchange server.
- Create a policy file that defines the spelling options for an Exchange server.
- Match a situation with the profile that is evaluated for use in that situation.
- Modify the System Policy Editor to use the Manual Update Mode.

## Unit 3: Managing Site Configuration

### Objectives:



- Identify the contents of the Add-Ins container.
- Match the additional containers within the Addressing container with their contents.
- Match the connector types included in the Connections container with the connectivity provided by them.
- Identify the contents of the Directory Replication container.
- Identify the functions of the monitors in the Monitors container.
- Match the Internet protocols in the Protocols container with the services they provide.
- Identify the contents of the Servers container.
- Change the SMTP address in the Site Addressing object of a site.
- Assign a value to a custom attribute of a recipient.
- Configure the Search Dialog details template.
- Assign the Search permission to a global group for a container in the Address Book View.
- Assign the Search permission to an Exchange Server site Service account for an Organization object.
- Pull the new directory information into a given Microsoft Exchange server site for another Microsoft Exchange server site.
- Match the DS Site Configuration object property pages with the options that can be configured through them.
- Match the Information Store Site Configuration object property pages with the options that can be configured through them.
- Match the MTA Site Configuration object property page with the options that can be configured through them.
- Match the Site Addressing object property pages with the options that can be configured through them.
- Configure directory object values for a site by using the DS Site Configuration object property pages.
- Enable message tracking on the MTA Site Configuration Object.

#### Unit 4: Managing Server Configuration

##### Objectives:

- Match the server configuration containers and objects in the server container with the tasks they perform.
- Identify the options to configure the properties of an Exchange server for a specific situation.
- Match the protocol objects in the Protocols container used to configure client connection behavior with their functions.

- Match the common tabs for configuring the Public Information Store with their functions.
- Match the tabs to configure a Private Information Store with their functions.
- Identify the options that can be configured through the property pages of the Directory Service object.
- Identify the options that can be configured through the property pages of the MTA object.
- Identify the options that can be configured through the property pages of the System Attendant object.
- Initiate the replication of directory entries within a site.
- Configure the Message Transfer Agent object of a server object by using Microsoft Exchange Administrator.
- Configure the System Attendant object of an Exchange server by using Microsoft Exchange Administrator.

**Microsoft Exchange Server 5.5 Concepts and Administration - Part 3**

Course 73363

*Produced by NETg*

**LEARN TO:**

- Identify public folder contents, create a public folder strategy, view and assign public folder permissions and set public folder affinity.
- Maintain a Microsoft Exchange Server Organization.
- Use the Exchange Server utilities to monitor Windows NT services on a computer and monitor the functioning of the network between two servers.
- Identify the types and features of collaboration applications.
- Create, modify and manage Exchange server forms.

**COURSE LENGTH:** 6 - 8 hour(s)

**Unit Names:**

Unit 1: Creating and Managing Public Folders

Objectives:

- Identify the features of the public folder components.
- Identify the advantages of the public folder strategies.
- Sequence the steps in creating public strategies.
- Create a public folder by using Microsoft Outlook.
- Send mail to a public folder by using Microsoft Outlook.
- Grant permissions to users for creating top-level public folders by using Microsoft Exchange Administrator.
- Configure public folder permissions by using Microsoft Outlook.
- Propagate the properties of a top-level folder to its subfolder by using the Microsoft Exchange

Administrator.

- Configure public folder replication by using the Replicas property page.
- Configure public folder site affinity by using Microsoft Exchange Administrator.
- Match the information store site configuration properties with the tasks they help you perform.
- Match the public information store properties with the tasks they help you perform.
- Sequence the steps for the flow of messages in a moderated folder.
- Sequence the steps for a folder event processing.

## Unit 2: Maintaining an Exchange Organization

Objectives:

- Match the Microsoft Exchange databases with their functions.
- Match the log files with their functions.
- Sequence the steps performed by Microsoft Exchange to manage the online backup operations of a split transaction.
- Identify the advantages of enabling database circular logging.
- Identify the benefits of storing log files separately from database files.
- Run the Microsoft Exchange Performance Optimizer by using the Microsoft Exchange Optimizer option.
- Display the performance optimizer log by using the Start button.
- Match the Exchange Server maintenance utilities with their functions.
- Match the database size maintenance methods with their uses.
- Identify the factors to be considered when planning a backup strategy.
- Select a backup strategy for a given scenario.
- Make a backup of the Microsoft Exchange Databases on a tape drive by using the Backup option.
- Identify the functions of the Exchange Server-specific switches.
- Identify the methods to verify the success of a backup event.
- Identify the other data that needs to be backed up in addition to Information Store and Directory Service.
- Identify the tests performed by the Inbox repair tool on personal folder files.
- Run MTACHECK by using the MTACHECK command.
- Identify the parameters that must be supplied to the RPC Ping utility.
- Identify the advantages of enabling message tracking.

- Track a message by using the Message Tracking Center window.
- Identify the maintenance tasks that need to be performed on the Exchange server.
- Configure the item recovery period on a private Information Store by using Microsoft Exchange Administrator.
- Recover deleted messages by using Outlook.

### Unit 3: Monitoring Microsoft Exchange Server

#### Objectives:

- Identify the functions of a server monitor.
- Identify the options for configuring the properties of a server monitor.
- Configure a server monitor by using Microsoft Exchange Administrator.
- Start the server monitor by using Microsoft Exchange Administrator.
- Identify the functions of a link monitor.
- Identify the options for configuring the properties of a link monitor.
- Configure a link monitor by using Microsoft Exchange Administrator.
- Start a link monitor using Microsoft Exchange Administrator.
- Configure a monitor to start automatically by using the Administrator program.
- Stop a monitor temporarily by using the Administrator program.
- Identify the methods to resolve message delays in MTA message queues.
- Match the options on the Internet Mail Service connector Queues page with their functions.
- Identify the functions of the Microsoft Mail Connector Queues page options.
- Match the Windows NT counters with their functions.
- Match the Microsoft Exchange Performance Monitor counters with their functions.
- Match the Microsoft Exchange performance charts with their functions.
- Configure the Performance Monitor to monitor communications between the servers within a site.
- Configure the performance monitor to send an alert message if the MTA queue length exceeds the specified value.

### Unit 4: Exchange Server Forms Administration

#### Objectives:

- Identify the functions of the components of a collaboration application.
- Match the types of collaboration applications with their features.

- Identify the Outlook application design features.
- Identify the Exchange Server features available to Outlook form applications.
- Identify the common roles and responsibilities of the personnel administering forms in an Organization.
- Identify the features of the forms stored in the various form libraries.
- Create an Organization forms library by using the Administrator Program.
- Create a form based on a standard Outlook form by using the Outlook Forms designer.
- Modify a form by using the Outlook Forms designer.
- Publish a form into a forms library by using the Outlook Forms designer.
- Associate a form with a public folder in Outlook.
- Access a form published in the Organization Forms library.

**Networking Technologies Series: ATM**

Course 12756

*Produced by NETg*

**LEARN TO:**

- Identify the functions of different technologies used to increase the network bandwidth.
- Describe the features of Asynchronous Transfer Mode (ATM).
- Describe how ATM works.
- Describe the issues involved in migrating to ATM.
- Describe issues involved with LAN emulation.
- Describe issues involved with integrating a WAN with ATM
- Identify the problems associated with legacy and virtual LANs.
- Identify the functions of virtual LANs
- Identify the features and advantages of routers in virtual LANs.
- Identify the features of Wide Area Networks, T-1 circuits, Packet Switched Networks, and Integrated Services Digital Networks.
- Describe the issues involved with implementation of ATM.

**COURSE LENGTH:** 7 - 8 hour(s)

**Unit Names:**

Unit 1: Asynchronous Transfer Mode: An Overview

Objectives:

- Identify the function of a full-duplex Ethernet
- Identify the functions of switching hub on an Ethernet LAN.
- Describe the functions of a switched Token Ring.
- Identify the features of a 100BaseT topology.
- Describe the features of 100VG-AnyLAN technology.

- Describe the features of a Fibre Channel technology.
- Describe the features of Asynchronous Transfer Mode (ATM).
- Identify the features of a User-to-Network Interface in a given ATM network.
- Identify the events that take place in an ATM virtual connection
- Match the fields of an ATM cell header with their functions.
- Sequence the steps in route determination.
- Describe the functions of an ATM switch in data forwarding.
- Identify the advantages of ATM.
- Describe the issues to be considered while migrating from protocol networks to ATM's switched environment.
- Describe the issues that make LAN emulation difficult to implement.
- Identify the issues to be considered while migrating desktops to ATM.
- Identify the issues to be considered before integrating WAN and ATM.
- Identify the limitations of ATM

## Unit 2: Virtual Network and ATM

### Objectives:

- Identify the functions of a collapsed backbone.
- Identify the problems associated with legacy LANs.
- Match the methods used to create virtual LANs with their features.
- Identify the advantages of using virtual subnet VLANs.
- Identify the features of an IP host-list VLAN.
- Identify the features of a rules-based virtual network.
- Identify the reasons for incorporating ATM backbones with Ethernet switches.
- Identify the problems associated with virtual networks.
- Identify the functions of a router.
- Identify the features of ATM edge routers.
- Identify the features of Multi-protocol over ATM (MPOA).
- Identify the reasons for incorporating policy-based management in VLANs.

## Unit 3: Wide Area Networks and ATM

### Objectives:

- Identify the features of a Wide Area Network.



- Identify the reasons for the unreliability of analog phone lines.
- Describe the advantages of T-1 circuits.
- Identify the functions of time division multiplexing.
- Identify the advantages of Ft-1 service.
- Identify the advantages of T-3 multiplexers.
- Sequence the steps involved in the operation of ATM.
- Sequence the steps involved in protocol translation.
- Identify the differences between X.25 packet-switching and T-1 multiplexing.
- Describe the functions of a multiplexer in a fast packet technology.
- Describe the functions of frame relay.
- Identify the features of Switched Multimegabit Data Service (SMDS).
- Identify the features of Basic Rate Interface (BRI).
- Identify the features of Primary Rate Interface (PRI).
- Identify the IEEE 802.9 standards.
- Describe the features of the Synchronous Optical Network (SONET).
- Identify the features of ATM PVC network interworking.
- Identify the features of Frame User to Network Interface (FUNI).
- Identify the functions of ATM Core and edge switches.

## **UNIX Advanced Topics**

Course 12672

*Produced by NETg*

### **LEARN TO:**

- Alter file formats of UNIX files using the various file transforming commands as well as the advanced UNIX tools
- Select an appropriate media for data backup and also perform backup and recovery of data.
- Understand the basic concepts and features of networking.
- Use the various UNIX networking commands.

**COURSE LENGTH:** 6 - 8 hour(s)

### **Unit Names:**

#### Unit 1: Transforming Files in UNIX

##### Objectives:

- Identify the need for file transformation.
- Replace the tab character with spaces using the expand command.
- Translate the case of text characters in a file using the tr command.
- Remove columns from a file using the colrm command:· Remove all columns after a certain column· Remove only a specific column
- Convert files from one format to another using the dd command:· Convert unblocked ASCII to ASCII format· Convert ASCII to unblocked ASCII format
- Identify the features of the awk utility.
- Identify the types of awk patterns:· Relation Expressions· Regular Expressions
- Display specific records from a file using the awk command.
- Create a new column in a file while assigning it a value using the nawk command.
- Identify the advantages of using sed.

- Identify the parts of the sed editing commands:· Addresses· Functions
- Replace a pattern globally with another in a file using the sed utility.

## Unit 2: Data Backup

### Objectives:

- Identify the benefits of data backup.
- Identify the features of various off-line backup media:· Floppy disks· Tapes
- Match the type of the floppy disk to its storage capacity:· 5¼ DS/DD Floppy Disks· 3½ DS/DD Floppy Disks· 5¼ DS/HD Floppy Disks· 3¼ DS/HD Floppy Disks
- Format a floppy disk using the format command.
- Identify the features of tapes.
- Erase all the previously stored data on a tape using the tapectl command.
- Specify the location of data storage on tapes using the mt command:· Forward the tape by file marks:· Rewind the tape.
- Backup a file using the tar command:· Append file to the end of the backup media:· Generate backup report.
- Generate a detailed list of the contents of backup media.
- Restore a file from the backup media using the tar command.
- Copying data to the archive medium using the cpio command in conjunction with the find command.
- Generate a list of the contents of backup media.
- Restore a file from the backup media using the cpio command.

## Unit 3: Networking Concepts and Commands

### Objectives:

- Identify the benefits of networking.
- Identify the features of a Local Area Network.
- Identify the features of a Wide Area Network.
- Identify the features of Ethernet.
- Identify the advantages of TCP/IP in internetworking.
- Match the protocols offered by TCP/IP with their functions.
- Identify the services provided by a file server to its clients.
- Identify the features of the file systems used for implementing distributed networking:· Network File System· Remote File System· Virtual File System

- Mount a remote file system using the mount command.
- Identify the prerequisites for accessing remote machines:· Login accounts· Special permission to users· Host names
- Log into a remote machine using the rlogin command:· Using your own account. · Using the different user's account.
- Display the status of a remote machine using the runtime command.
- Display the list of users logged on to the local network, using the rwho command.
- Copy files remotely using the rcp command: From remote machine to the local machine.· From local machine to the remote machine.
- Display system information on a remote machine using the rsh command: Display the current time on a remote machine. Display the disk space on a remote machine.
- Copy files from one UNIX system to another using the uucp command.
- Transfer files from one remote machine to another using the ftp command.
- Transfer files from one system to another using the tftp command.
- Log in to a remote machine using the telnet command.
- Identify the features of GUI.
- Identify the features of the X Windows system such as GUI, flexibility, portability and network transparency.
- Match the commands used in X Windows with their functions.

## **Unix Shell Programming**

Course 12777

*Produced by NETg*

### **LEARN TO:**

- Manage UNIX files and directories using the UNIX shell commands.
- Work with shell variables, metacharacters and regular expressions.
- Use shell commands to redirect input, output and error messages, and archive files in the background.
- Write different types of shell scripts.
- Program in the Korn Shell environment.

**COURSE LENGTH:** 7 - 8 hour(s)

### **Unit Names:**

Unit 1: Introduction to the Bourne Shell

Objectives:

- Identify the functions of a shell.
- Define a shell.
- Identify the features of three different types of shells.
- Match the UNIX directories with the files they contain.
- Determine the three sets of permissions on a file using the ls command.
- Change the permissions on a file using the symbolic method of chmod command.
- Create a file using the cat command.
- Copy one file to another using the cp command.
- Compare two ASCII files using the diff command.
- Delete files using the rm command.
- Sort the items stored in a file according to a given pattern.

- Change the current working directory using the full pathname.
- Create a sub-directory under a directory that does not exist.
- Delete a directory using the rmdir command.
- Copy the entire directory structure present under the current working directory into another.

## Unit 2: Variables, Metacharacters and Expressions

### Objectives:

- Work with shell variables to modify your environment.
- Given a value, assign it to a shell variable.
- Change the command-line prompt using PS1.
- List filenames using a combination of metacharacters.
- Assign the output of one command to another using the back quote character.
- Match the pattern-matching operators with their functions.
- Search for a pattern using the grep command.
- Remove blank line in a file using grep command.

## Unit 3: File Input and Output

### Objectives:

- Redirect the contents of two files to a third file using the cat command.
- Redirect the standard input to the wc command from a named file.
- Search for the names of all the files created or modified on a particular date using pipes.
- Redirect the output of a command to a file using the tee command.
- Redirect an error message using a file descriptor.
- Create an archive file by grouping commands.
- Process grouped commands in the background.

## Unit 4: Shell Scripts

### Objectives:

- Given a file with a shell script entered, convert it into an executable file.
- Execute a shell script using command line processing.
- Write a shell script to perform integer arithmetic.
- Write a shell script using if-then-else statements.

- Write a shell script using case statement.
- Write a shell script using the for loop.
- Write a shell script using the while loop.
- Write a shell script to read a value input by a user.
- Given the options to be displayed and the response, write a menu-driven script.
- Write script to extract data from a file using the cut command.
- Write a script to paste the contents of a file using the paste command.
- Write a script to edit the contents of a file using the sed command.
- Write a shell script to interrupt a process using the trap command.

#### Unit 5: Korn Shell Programming Extension

##### Objectives:

- Identify the features of the Korn shell.
- Given a range, display a list of commands from the command history list.
- Given that a job is being performed in the foreground, suspend the job.
- Restore the initial value of a variable using the typeset command.
- Identify the Built-In commands of the Korn shell.
- Create a menu using the select statement.
- Given a command, create an alias for it.
- Write a shell script to reverse the order of an array of 10 elements in it.

## **UNIX SVR4 System Administration Fundamentals**

Course 12778

*Produced by NETg*

### **LEARN TO:**

- Identify the pre-installation procedures and install a UNIX system.
- Identify the UNIX startup and shutdown processes.
- Create and manage UNIX file systems.
- Work with system resources.
- Set up and administer user accounts.
- Set up system accounting and identify the information tracked by different types of accounting.

**COURSE LENGTH:** 7 - 8 hour(s)

### **Unit Names:**

Unit 1: UNIX Installation Basics

Objectives:

- Identify the different types of UNIX systems and users.
- Match the UNIX systems with their features.
- Identify the tasks performed by UNIX users.
- Match the system names in UNIX with their uses.
- Identify the features of UNIX slices and file systems.
- Identify the advantages of multiple file systems.
- Match the UNIX slices with their features.
- Match the UNIX file systems with their features.
- Install a UNIX system.
- Sequence the steps to boot a UNIX system from a local CD-ROM.



## NMCI Security Policy

- Configure a UNIX system.
- Install a UNIX server.
- Install a given package using the admintool.

### Unit 2: Booting the Server

#### Objectives:

- Sequence the processes that are initiated on booting the system.
- Log into a UNIX server as a super-user.
- Identify the features of a startup script.
- Match the UNIX system states to their features.
- Change the system state using the init command.
- Match the run control scripts with their functions.
- Shut down the system using the shutdown command.

### Unit 3: File System Administration

#### Objectives:

- Identify the types of files systems and their parameters.
- Create and label a file system.
- Match the components of a file system with their features.
- Match the file system parameters with their features.
- Create a file system using the newfs command.
- Label a file system using the labelit command.
- Mount and unmount file systems in UNIX.
- Mount a file system using the mount command.
- Unmount a file system using the unmount command.
- Match the functions of fsck with the phase in which they are performed.
- Check a ufs file system using the fsck command.
- Find free disk space using the df command.
- Search for files using the find command.

### Unit 4: Device Administration

#### Objectives:

## NMCI Security Policy

- Identify the steps in the SAF initialization process.
- Identify the functions of the components within SAF.
- Complete the sacadm command to create a port monitor.
- Given a port monitor, display its status using the sacadm command.
- Enable a port monitor using the sacadm command.
- Given the parameter, complete the pmadm command to create a port service.
- Display the status of a port service linked to a given port monitor tag using the pmadm command.
- Enable a port service by using the pmadm command.
- Set up the local printing services using the lpadm command.
- Complete the code to set up the print server using the print server commands.
- Given the name of the client printer, configure it using the lpadm command.
- Identify the features of the components on which X architecture is based.
- Match the X resources command line options with what they specify.
- Match the xdm configuration files with their features.
- Identify the performance related factors required before installing PC X servers.

## Unit 5: User Administration

### Objectives:

- Match the components of a user account with their description.
- Add a user account using the admintool.
- Modify a user account using the admintool.
- Disable a user account using the admintool.
- Remove a user account using the admintool.

## Unit 6: UNIX Server Accounting

### Objectives:

- Identify the system information that is tracked by UNIX system accounting.
- Sequence the steps involved in the system accounting process.
- Set up system accounting to run when the system is in multi-user state.
- Identify the information tracked by connect accounting.
- Identify the information tracked by process accounting.
- Identify the information tracked by disk accounting.

## NMCI Security Policy

- Identify the information tracked by fee calculations.

**Networking Technologies Series: Network Security**

Course 12764

*Produced by NETg*

**LEARN TO:**

- Identify security threats.
- Identify tools for protecting networks.
- Describe methods of implementing LAN security.
- Identify threats to system security.
- Describe strategies for protecting system security.

**COURSE LENGTH:** 6 - 8 hour(s)

**Unit Names:**

Unit 1: Security Threats and Prevention

Objectives:

- Identify the general network security threats and the tools for reducing network and database security threats.
- Identify the reasons for LANs vulnerability to security threats.
- Identify system and personnel policies for reducing security threats.
- Identify the types of computer viruses.
- Identify the damages caused by a virus to a system.
- Identify the functioning of boot sector and file viruses.
- Identify the features of polymorphic and stealth viruses.
- Describe the types of computer malware.
- Identify the types of anti-virus software.
- Identify the functions of virus scanner, integrity checker and behavior blocker anti-virus programs.

## Unit 2: Implementing LAN Security

### Objectives:

- Identify the safeguards that prevent physical access threats to a LAN.
- Match the physical access safeguards that detect threats with their function.
- Match the physical access safeguards for containing security threats with their examples.
- Match the safeguards that establish employee accountability for physical LAN access with their functions.
- Identify the safeguards that prevent, detect, correct and establish responsibility for electronic network threats.
- Match the electronic network safeguards with their role in preventing security threats to LANs.
- Identify the electronic network threat detection safeguards.
- Identify the electronic network safeguards for establishing employee accountability.
- Match the management control safeguards that prevent threats to LANs with their roles.
- Match the management control safeguards for detecting threats to LANs with their roles.
- Identify the management control safeguards that help in containing threats.
- Identify the management control safeguards that establish employee accountability.

## Unit 3: System Security

### Objectives:

- Identify the risks to system security.
- Identify the strategies used to counter risks to the network system.
- Identify the components of a security analysis of the network.
- Identify various strategies to protect a system: Access control, authentication, passwords, encryption, biometrics, modem security, and firewalls.
- Match methods of authenticating users with their functions: Authentication by Possession, authentication by intrinsic characteristics, authentication by knowledge.
- Describe guidelines for choosing effective passwords.
- Match biometric analyses with their function: Fingerprint analysis, handprint analysis, voice pattern analysis, handwriting analysis, keystroke analysis, and retina scans.
- Identify the ways of preventing illegal access to a network through modem dial-ups.
- Describe the functions of a firewall.
- Identify the various techniques used to disguise data in order to protect it from unauthorized users.
- Identify the features of the public/private key encryption technique.

## NMCI Security Policy

- Sequence the steps involved in the Kerberos authentication process.
- Identify the features of Pretty Good Privacy.
- Match the methods of masking data with their functions: Electronic signature, clipper, compression, padding, and lost in a crowd.

## Implementing Security for Web Sites - Part 1

Course 12700

**Produced by NETg**

### **LEARN TO:**

- Manage Internet security.
- Gain access and secure the gateway.
- Create a secure messaging channel.
- Address security risks associated with Java, CGI and Viruses.

**COURSE LENGTH:** 6 - 8 hour(s)

### **Unit Names:**

Unit 1: Managing Internet Security

Objectives:

- Exploring addresses, subnets and hostnames.
- Working with network interfaces.
- Reviewing the network configuration files.
- Understanding the network access files.
- Examining TCP/IP Daemons.
- Exploring TCP/IP Utilities.
- Examining the System Daemons.
- Creating Daemons with the Bourne Shell.
- Creating Daemons with PERL.
- UNIX Run Levels.
- The UUCP Network.
- Naming your Host.
- The System V basic networking utilities UUCP.

## NMCI Security Policy

- The UUCP chat script.
- Configuring Version 2 UUCP.
- Configuring UUCP over TCP/IP.
- Audit trails under UNIX.
- Audit trails under Windows NT.
- Audit trails under DOS.
- Using system logs to discover intruders.

## Unit 2: Gaining Access And Securing the Gateway

### Objectives:

- Sniffing.
- Spoofing.
- How to build a firewall:
- The TIS Firewall Toolkit
- Preparing for configuration
- Configuring TCP/IP
- The netperm table
- Configuring netacl
- Configuring the Telnet Proxy
- Configuring the rlogin gateway
- Configuring the FTP gateway
- Configuring the Sendmail proxy: smap and smapd
- Configuring the HTTP proxy
- Configuring the X Windows Proxy
- Understanding the authentication server
- Using plug-gw for other services
- The companion administrative tools
- SATAN
- The nature of network attacks
- Thinking like an intruder
- Introduction to SATAN
- Detecting SATAN



## NMCI Security Policy

- Using secure network programs
- SSL
- Investigating what SATAN does
- Building SATAN
- Kerberos
- How Kerberos works
- The Kerberos network
- How authentication works
- Encryption
- Versions of Kerberos
- Selecting a vendor
- Vendor interoperability issues
- Naming constraints
- Cross-realm operation
- Ticket flags
- Message exchanges
- Kerberos workstation authentication problem

## Unit 3: Messaging Security

### Objectives:

- What is encryption?
- Transposition.
- Substitution.
- PGP:

### Overview

### How to use PGP

### PGP keys

### Key management

### Basic message operations

### Advanced message operations

### The PGP configuration file

Unit 4: Newer Concerns and Issues

Objectives:

- Java security issues.
- Setting up Java security features.
- Understanding CGI and HTTP security risks.
- Minimizing CGI and HTTP security risks.
- Bypassing CGI.
- Server Side Includes (SSI).
- Other Language Issues.
- Computer Viruses: most likely targets.
- IBM PC computer virus types.
- Network and virus susceptibility.
- Virus classes.
- How antivirus programs work.
- Preventative measures and cures.

## **Implementing and Administering Web Servers - Part 1**

Course 12703

### **7.0 Produced by NETg**

#### **LEARN TO:**

- Identify the features of a Web server.
- Select a Web server according to business needs.
- Set up a Web server successfully.
- Understand basic Web Server Configuration.
- Access security features for the Web Server.
- Understand the attributes of CGI programs.
- Learn to operate a database.

**COURSE LENGTH:** 7 - 8 Hours

#### **Unit Names:**

Unit 1: Web Server Selection and Installation

Objectives:

- Select a Web Server according to business needs.
- Know the features of a Web server.
- Select a suitable server.
- Understand the requirements to install the Netscape Enterprise server.
- Install the server software.
- Know the administration server options that are configured on the Netscape Enterprise server.
- Using the Server Selector window, implement the initial configuration of the Netscape Enterprise server.

Unit 2: Web Server Configuration

### Objectives:

- Describe the main components of System Settings.
- Recognize the components of content management.
- Learn about security issues and solutions in Web Site management.
- Identify the technical settings that influence server performance.
- Identify the network settings that are configured on a server.
- Identify the ways in which to manage content.
- Use Server Manager to set the primary document directory on the Netscape Enterprise server.
- Use Server Manager to create access to a user directory on the Netscape Enterprise server.
- Match the factors responsible for data request management with their functions.
- Match the configuration styles with their functions.
- Define configuration styles.
- Explore possible solutions to the main security issues connected with administering a Web site.
- Identify the methods to implement security in a Website.
- Create a user database on the Netscape Enterprise server using Server Manager.
- Create access for users on the Netscape Enterprise server using Server Manager.
- Create access restriction.
- Match the types of special access with their potential risks.
- Recognize the features of Firewalls and Proxy Servers.
- Identify the methods by which Firewalls ensure Website security.
- Identify the Network access policies that influence a Firewall.
- Match the special security features with their functions.
- Identify the feature of a Proxy server.
- Know the guidelines for building a Firewall.
- Learn about technical and content settings of a server and security issues and solutions.

### Unit 3: Advanced Web Server Configuration

#### Objectives:

- Know the features, installation procedures and working of Common Gateway Interface.
- Identify the security concerns while using CGI on your Web server.

- Know the features of Common Gateway Interface.
- Install the CGI program on the Netscape Enterprise server using the CGI Directory method from the Server Manager window.
- Sequence the steps involved in the working of CGI programs.
- Match the security concerns with their solutions.
- Match the server-side applications with their features.
- Monitor a server using log files.
- Set log preferences using the Server Manager on the Netscape Enterprise server.
- View the log files using the Server Manager on the Netscape Enterprise server.
- Generate server statistics using the log analyzer on the Netscape Enterprise server from the Server Manager Window.
- Implement the various advanced services provided by the Web server.
- Match the tasks to be performed to manage collections with their results.
- Match the components required to customize the text search interface with their functions.
- Identify the functions of a catalog agent.
- Operate a Database with CGI and Third Party Tools.
- Identify the functions of a CGI program in database integration.
- know the features of Third Party Tools.
- Match the Web server application with the database integration facility it provides.
- Identify the tasks associated with administrating a database at a Website.

LEVEL III

**System Administrator Level 3 Certification Criteria**

**System Administrator Level 3 Certification requires the following technical training, IA training, and on-the-job experience:**

- **Level 2 certification**  
**and**
- **Formal technical training equivalent to Level 3 Technical Training Minimum Standards<sup>1</sup>**  
**and**
- **Completion of Navy Information Systems Security Manager (ISSM) Course (NEC 2779) OR System Administrator Level 3 Incident and Accreditation Awareness video/CBT<sup>2</sup>**  
**and**
- **Formal IA training equivalent to Level 3 Information Assurance Training Minimum Standards<sup>3</sup>**  
**and**
- **5 years System Administrator experience**

**8.0 Notes**

**<sup>1</sup> Level 3 Technical Training Minimum Standards**

**Formal technical training in the following areas:**

- **advanced installation, configuration, troubleshooting, and management of Windows NT system in an enterprise environment**
- **advanced analysis and optimization of the Windows NT server subsystems**
- **advanced analysis and optimization of Windows NT network performance**
- **network protocols**
- **configuration and management of TCP/IP on Windows NT 4.0**

- **advanced configuration and optimization of Microsoft Exchange Server 5.5**
- **heterogeneous network integration and optimization**
- **advanced management and optimization of UNIX server environments**

### **Equivalent CNET Schools**

**CNET Advanced Network Analyst (ANA) Course (NEC 2781)**

**Equivalent NETg Technical Training COI for Level 3**

<b><u>Course #</u></b>	<b><u>Course Title</u></b>
71415	MS Windows NT 4.0 Server Analysis and Optimization
71416	MS Windows NT 4.0 Server Network Analysis and Optimization- Part 1
71417	MS Windows NT 4.0 Server Network Analysis and Optimization - Part 2
71418	Troubleshooting Microsoft Windows NT Server 4.0 in the Enterprise Environment
71419	Installing and Configuring Microsoft Windows NT Server 4.0 in the Enterprise Environment - Part 1
71420	Installing and Configuring Microsoft Windows NT Server 4.0 in the Enterprise Environment - Part 2
12773	Networking Technologies Series: TCP/IP Internetwork Management
71435	Internetworking Microsoft TCP/IP on Microsoft Windows NT 4.0 - Part 1
71436	Internetworking Microsoft TCP/IP on Microsoft Windows NT 4.0 - Part 2
71437	Internetworking Microsoft TCP/IP on Microsoft Windows NT 4.0 - Part 3
71438	Internetworking Microsoft TCP/IP on Microsoft Windows NT 4.0 - Part 4
73365	Microsoft Exchange Server 5.5 Design and Implementation - Part 1
73366	Microsoft Exchange Server 5.5 Design and Implementation - Part 2
73367	Microsoft Exchange Server 5.5 Design and Implementation - Part 3
73368	Microsoft Exchange Server 5.5 Design and Implementation - Part 4
73369	Microsoft Exchange Server 5.5 Design and Implementation - Part 5
12763	Networking Technologies Series: Managing Multivendor Networks
12779	UNIX SVR4 System Administration Advanced Topics

*Total of 18 classes, approximately 125 hours of training.*



<sup>2</sup> SA Level 3 Incident and Accreditation Awareness video/CBT to be developed and distributed in FY00

### 9.0 <sup>3</sup> Level 3 Information Assurance Training Minimum Standards

Formal IA training in the following areas:

- identification of factors that affect data integrity
- identification of the methods to improve data integrity and fault tolerance
- identification of backup system components and types of backup strategies
- identification of different methods to prepare for disaster recovery
- disaster recovery methodology
- various encryption methods
- identification of Pretty Good Privacy (PGP) features and the various security measures
- identification of the threats associated with the Web
- identification of the risks associated with Web clients and servers
- identification of the measures and issues related to CGI and HTTP security
- identification of the different types of viruses and antivirus programs and how they work

Equivalent CNET Schools

None

Equivalent NETg IA COI for Level 3

<u>Course #</u>	<u>Course Title</u>
12765	Data Integrity
12701	Web Site Security - Part 2

## **Microsoft Windows NT Server 4.0 Analysis and Optimization**

Course 71415

*Produced by NETg*

### **LEARN TO:**

- Identify the features of Windows NT server resources, Performance Monitor, and the techniques for server analysis and optimization.
- Create a measurement baseline by collecting data, creating log files and viewing the reports of the log files.
- Monitor system objects to detect various system bottlenecks, identify the issues to be considered for setting expectations from Windows NT server and determine the need for an additional server.
- Identify the system bottlenecks and resource implications in different environments.

**COURSE LENGTH:** 6 - 8 hour(s)

### **Unit Names:**

Unit 1: Basics of Server Analysis and Optimization

Objectives:

- Identify the features of virtual memory.
- Match the components affecting disk subsystem with their impact on the Windows NT server performance.
- Identify the factors that affect the network performance.
- Match the tools for server analysis and optimization with their functions.
- Identify the options provided by Performance Monitor.
- Match the Performance Monitor objects with their descriptions.
- Identify the Performance Monitor view that should be used to display the data:

Chart View

Alert View

## Report View

## Log View

- Set alerts on Performance Monitor, given the Add to Alert dialog box.
- Identify the techniques for server analysis and optimization, and sequence the steps for server analysis and optimization.

## Unit 2: Implementing a Measurement Baseline

### Objectives:

- Collect system data using the at command.
- Generate measurement baseline data, given the Add to Log dialog box of Performance Monitor.
- Create a new log file to serve as a measurement database, given the Add to Log dialog box of Performance Monitor.
- Export a log file to an Excel worksheet using Performance Monitor.

## Unit 3: Monitoring, Forecasting and Record Keeping

### Objectives:

- Create a report to detect the system bottleneck using Performance Monitor.
- Identify the counter causing the processor bottleneck, given the Performance Monitor chart.
- Create a chart to detect the counter causing the processor bottleneck using Performance Monitor.
- Identify the counter causing the processor bottleneck, given the Performance Monitor chart.
- Create a chart to detect the counter causing the memory bottleneck using Performance Monitor.
- Identify the counter causing a disk subsystem bottleneck, given the Performance Monitor chart.
- Create a chart to detect the counter causing the disk subsystem bottleneck using Performance Monitor.
- Create a chart to identify the counter causing network bottleneck using Performance Monitor.
- Identify the issues to be considered for defining response expectations from Windows NT.
- Sequence the steps to ascertain whether an additional Windows NT server is needed.
- Identify the information to be included in server analysis and optimization documentation.

## Unit 4: System Performance in Different Environments

### Objectives:

- Identify the workload units for a file and print server environment.

- Identify the object to be monitored in a given file and print server environment.
- Identify the factors that influence forecasting in a file and print server environment.
- Sequence the steps to calculate the number of users a file and print server can support.
- Change the configuration setting of the file and print server to maximize RAM, given the Control Panel.
- Identify the workload units for an application server.
- Create a chart to detect the system bottleneck using Performance Monitor in a given client/server application environment.
- Identify the solutions to remove system bottlenecks in an application server environment:

Memory

Disk

Processor

Network

- Sequence the steps to calculate the number of users an application server can support.
- Change the configuration settings of an application server to maximize RAM, given the Control Panel.
- Identify the workload units for domain server.
- Identify the impact of the domain server environment on the system resources:

Memory

Disk

Processor

Network

- Identify the factors to be considered when forecasting in a domain server environment.
- Identify the factors that influence the number of users a domain server can support.

**Microsoft Windows NT Server 4.0 Network Analysis and Optimization - Part 1**

Course 71416

*Produced by NETg*

**LEARN TO:**

- Analyze network traffic in a Microsoft Windows NT environment.
- Be introduced to Microsoft Network Monitor, a Windows NT network traffic data capturing and analyzing tool.
- Analyze and optimize the client initialization traffic in a Windows NT environment.
- Analyze and optimize the client-to-server traffic in a Windows NT environment.

**COURSE LENGTH:** 6 - 8 hour(s)

**Unit Names:**

Unit 1: Windows NT Network Traffic Analysis

Objectives:

- Identify the benefits provided by network traffic analysis to a network administrator in a Windows NT environment.
- Identify the guidelines to characterize a Windows NT service.
- Identify the features of the elements of network traffic.

Unit 2: Network Traffic Analyzing Tool

Objectives:

- Identify the uses of Microsoft Network Monitor.
- Install the simple version of Microsoft Network Monitor on the Windows NT server.
- Match the Capture Window panes of the Microsoft Network Monitor interface with the data they display.
- Capture the network traffic data with Microsoft Network Monitor.
- Identify the data displayed by the three panes of the Network Monitor Capture Summary Window of Microsoft Network Monitor.

### Unit 3: Windows NT Client Initialization Traffic

#### Objectives:

- Identify the network activities that generate different types of client initialization traffic in a Windows NT environment.
- Identify the function of the two phases that generate traffic in a DHCP client-to-server interaction process.
- Identify the frames that generate network traffic in IP address lease.
- Identify the frames generated in the renewal of the IP address from the DHCP.
- Configure the duration of IP address leases to a specified time limit using the DHCP manager.
- Identify the processes that generate network traffic in a WINS client-to-server interaction.
- Identify the frames generated in the name registration and renewal process.
- Identify the frames generated in the name resolution process.
- Identify the frames generated in the name release process.
- Configure the renewal interval of WINS clients to a specified time limit using the WINS manager.
- Identify the cause of the network traffic in a file session.
- Sequence the steps that take place to establish a file session in a Windows NT environment.
- Identify the frames generated in a session connection.
- Identify the frames generated during session termination process.
- Identify the methods to control the network traffic generated by file sessions in a Windows NT environment.
- Identify the causes of the network traffic generated by logon validation.
- Identify the steps of the two processes that generate traffic while locating a logon server:

Broadcasting to NetLogon process.

Using WINS process.

- Sequence the network activities that generate traffic while validating the logon request of a Windows 95 and a Windows NT client.
- Identify the methods that determine the number of domain controllers to optimize the logon validation process.

### Unit 4: Windows NT Client-To-Server Traffic

#### Objectives:

- Be introduced to the types of client-to-server traffic generated in a Windows NT environment.

- Identify the definition of client browsing.
- Identify the frame generated in the host announcement process.
- Identify the features of the traffic generated during the retrieval of a browse list.
- Identify the methods used to control the network traffic generated by the client browsing process.
- Identify the causes that generate Domain Name System (DNS) traffic in a Windows NT environment.
- Identify the frames generated in the two-way process of DNS lookup:  
Client request.  
Server response.
- Identify the frames generated in the DNS recursive lookup process.
- Identify the methods to optimize DNS traffic in a Windows NT environment.
- Configure the time to live (TTL) for all records of a zone to a specified time limit using DNS Manager.
- Configure TTL for an individual record of a specified zone using DNS Manager.
- Configure TTL for WINS Record to a specified time limit using DNS Manager.
- Identify the causes that generate traffic during intranet browsing.
- Sequence the steps that generate traffic while connecting to a web site.
- Identify the guidelines to optimize intranet browsing traffic.

**Microsoft Windows NT Server 4.0 Network Analysis and Optimization - Part 2**

Course 71417

*Produced by NETg*

**LEARN TO:**

- Analyze and optimize Windows NT 4.0 server-to-server network traffic to establish an effective enterprise network.
- Identify the network traffic generated in various scenarios in a Windows NT 4.0 environment.

**COURSE LENGTH:** 4 - 6 hour(s)

**Unit Names:**

Unit 1: Windows NT Server-to-Server Network Traffic

Objectives:

- Match the processes that generate server-to-server traffic on the Windows NT 4.0 network with their uses.
- Sequence the frames generated during the different phases of the Account synchronization process.
- Sequence the steps in which the Accounts database of the backup domain controller is updated.
- Sequence the steps in which the trusting domain controller adds a trusted domain to establish a trust relationship.
- Sequence the steps used by the trusting domain controller to import trusted accounts.
- Identify the ways in which the group accounts can be used to optimize the trust relationship traffic between the domains.
- Analyze and optimize the traffic generated by browsing in a Windows NT environment.
- Sequence the steps in which traffic is generated when establishing a relationship between the WINS replication partners.
- Identify the maximum number of bytes generated on the network when updating records in the WINS database.
- Identify the best configuration option to optimize the WINS replication traffic for a given situation on the network.



- Sequence the steps involved in the traffic generated by the Directory Replicator service in a Windows NT environment and optimize the Directory Replicator traffic.
- Sequence the steps involved in the process of the DNS replication of the zone information in a Windows NT environment.
- Optimize the DNS server-to-server traffic by altering the default values to the Control parameters.

## Unit 2: Windows NT 4.0 Network Traffic

### Objectives:

- Identify the set of variables to be considered during the implementation of various network services.
- Identify the formula to speculate the total network traffic in a Windows NT 4.0 environment.
- Identify the traffic generated by the processes of the DHCP service, DHCP lease acquisition traffic, DHCP lease renewal traffic.
- Match the different processes of the domain controllers in a single domain LAN with the network traffic they generate.
- Match the network processes that occur during accounts trusting in a multiple domain LAN with the traffic generated by them.
- Identify the way to reduce the logon validation traffic in a WAN environment.

## **Troubleshooting Microsoft Windows NT Server 4.0 in the Enterprise Environment**

Course 71418

*Produced by NETg*

### **LEARN TO:**

- Identify the troubleshooting methodology, functions of the Kernel Mode networking components and Distributed networking Components.
- Identify the registry structure, subtrees and configuration information about a local machine.
- Identify the functions of the processes in every boot phase and troubleshoot through system files.
- Match the stop screen sections and parameters with their contents and use various debugging utilities.
- Identify types of startup errors and troubleshoot disk related and configuration problems.
- Troubleshoot RAS problems, resource access and permission problems, recover a mirror set and stripe set with parity.

**COURSE LENGTH:** 5 - 7 hour(s)

### **Unit Names:**

Unit 1: Troubleshooting from an Architectural Perspective

Objectives:

- Identify the steps of the troubleshooting methodology and the components of the Windows NT executive.
- Identify the function of the Windows NT Architectural layers.
- User Mode.
- Kernel Mode.
- Identify the functions of the Kernel Mode components in Windows NT Executive, Executive Services Layer, Microkernel Layer, Hardware Abstraction Layer.
- Identify the functions of the Distributed Networking components of the Networking Architecture.

## Unit 2: Modifying the System through the Registry

### Objectives:

- Match the Windows NT components with the way in which they use the information stored in the registry.
- Match the registry subtrees with the information they store.
- Display a registry subkey content using the Registry Editor.
- Set up an interactive session to troubleshoot through a remote Windows NT server registry, using the remote command service.
- Match the HKEY\_LOCAL\_MACHINE subtree to the information they store.
- Match the HKEY\_LOCAL\_MACHINE\HARDWARE subtrees with their functions.
- Identify the subkeys of HKEY\_LOCAL\_MACHINE\SYSTEM.
- Match the subkeys of CurrentControlSet to their functions.
- Match the CurrentControlSet\Services value entries to their functions.
- Match the CurrentControlSet\Services value names with their functions.
- Troubleshoot the problem using the Drives Utility, given that a service has failed to initialize.
- Troubleshoot service problems using the services subkey value entries.

## Unit 3: Boot Failures: Troubleshooting

### Objectives:

- Match processes in every boot phase to their functions, Initial Phase, Boot Loader Phase, Kernel Phase, Logon Phase.
- Set the parameters in the Boot.ini file using the system editor, Timeout, Default.
- Match the Boot.ini switches with their functions.
- Match the column names of the DRIVERS utility to the information they display.
- Enable event logging using the Registry Editor.
- Match the Emergency Repair Process options to their functions.
- Replace corrupted files using the Expand-R command.
- Create an Emergency Repair Disk.
- Create a disk to use the Windows NT hardware detection tool.
- Display registry information, using the Windows NT diagnostics administrative tool.
- Display hardware components using the debug version of Ntdetect.com.
- Display Windows NT compatible hardware using the hardware query tool.

#### Unit 4: Stop Screens and Debugging Utilities

##### Objectives:

- Match the stop screen sections with their contents.
- Match the stop screen parameters with the information they display.
- Match the debugging terms with their descriptions.
- Match the debugger types with their features.
- Identify the functions of the debug setup methods.
- Configure the Windows NT Kernel Debugger.
- Setup the Windows NT Kernel Debugger for remote access.
- Configure Windows NT system to store the content of a stop screen in a dump file and use the following Utilities, DumpCheck, DumpExam, Dr. Watson.

#### Unit 5: Troubleshooting System Problems

##### Objectives:

- Identify the types of startup problems on x86 systems.
- Troubleshoot system partition problems using the FDISK utility.
- Display the Master Boot Record using the DiskProbe utility.
- Display the Partition Boot Sector using the DiskProbe utility.
- Identify the causes of CMOS problems.
- Identify the types of problems that are rectified using the LastKnownGood configuration.
- Match the post logon disk problems with their solutions.

#### Unit 6: Troubleshooting Connectivity and Resource Access Problems

##### Objectives:

- Create a DEVICE.LOG file to troubleshoot modem problems using the Registry Editor.
- Create a PPP.LOG file to solve authentication problems using the Registry Editor.
- Match the error messages related to port problem with their solutions.
- Match the printer problems with their solutions and the permission problems with their solutions.
- Sequence the steps to construct the mirror set.
- Sequence the steps to reconstruct a stripe set with parity.

## **Installing and Configuring Microsoft Windows NT Server 4.0 in the Enterprise**

Course 71419

*Produced by NETg*

### **LEARN TO:**

- Install and configure a Windows NT Server.
- Configure and Manage Hard Disks, Printers and Windows NT Server for Client Computers.
- Install and configure Internet services and Remote Access Service.

**COURSE LENGTH:** 6 hour(s)

### **Unit Names:**

#### Unit 1: Installing and Configuring the Server

##### Objectives:

- Identify the minimum hardware requirements for installing Windows NT Server 4.0.
- Install the file system on a Windows NT Server 4.0.
- Configure a Windows NT Server 4.0 as a domain controller.
- Configure the network environment for the Windows NT Server installation.
- Configure the Windows NT Server environment.
- Identify the situations suitable for configuring TCP/IP on a Windows NT Server 4.0.
- Identify the situations suitable for configuring TCP/IP with DHCP on a Windows NT Server 4.0.
- Identify the situations suitable for configuring TCP/IP with WINS on a Windows NT Server 4.0.
- Identify the situations suitable for configuring the NWLink IPX/SPX Compatible Transport Protocol on a Windows NT Server 4.0.
- Identify the situations suitable for configuring the Data Link Control (DLC) protocol on a Windows NT Server 4.0.
- Identify the situations suitable for configuring the Apple Talk protocol on a Windows NT Server 4.0.

- Configure the advanced options of the TCP/IP protocol on a Windows NT Server:  
Set the IP Address.  
Set the subnet mask.  
Modify the gateway setting.
- Configure the TCP/IP protocol on a Windows NT domain controller using the DHCP server.
- Configure the NWLink IPX/SPX Compatible Transport protocol on a Windows NT Server.
- Modify the internal network number.
- Add frame types to network adapters.
- Enable RIP routing.
- Configure the protocol bindings for the Data Link Control (DLC) protocol.
- Configure the AppleTalk protocol on a Windows NT Server.
- Install and configure multi-protocol routing to server as Internet router, DHCP Relay Agent and IPX router.
- Configure the Directory Replicator service at a domain controller to start automatically.
- Configure the Directory Replicator service between two domain controllers.
- Configure the Windows NT Server to perform as a Preferred Master Browser.

## Unit 2: Configure NT Server Components

### Objectives:

- Identify the features of a RAID disk configuration.
- Identify the features of Stripe Sets.
- Identify the features of Mirror Sets.
- Identify the guidelines for configuring Mirror Sets.
- Identify the guidelines for configuring Stripe Sets with Parity.
- Create a Stripe Set to improve the performance of the Server.
- Create a Stripe Set with Parity to provide redundancy.
- Make a directory shareable.
- Assign the Read permission to a shared directory.
- Revoke the sharing of a directory.
- Configure a local printer.
- Set up a remote printer.
- Create a printer pool.
- Configure a NetWare-based printer with specific settings.

## NMCI Security Policy

- Set the highest priority for a printer.
- Identify the functions of the Network Client Administrator.
- Configure the Windows NT Server for Windows-based clients.
- Administer remote servers from client computers, Windows 95 Computers, Windows NT Workstation.

### Unit 3: Setting up the Internet

#### Objectives:

- Install the Internet Information Server.
- Configure the Internet Information Server through the various views of the Microsoft Internet Service Manager:

Pause a service.

Start a Service.

Connect to a server.

- Configure the World Wide Web service properties on the Internet Information Server:

Set the password.

Allow browsing rights.

- Activate the Domain Name Service on the Windows NT Server.
- Configure the Domain Name Service (DNS) on the Windows NT Server.
- Identify the benefits of integrating Intranet with Internet technology.

## **Installing and Configuring Microsoft Windows NT Server 4.0 in the Enterprise**

Course 71420

*Produced by NETg*

### **LEARN TO:**

- Configure Windows NT server for interoperability with a NetWare server.
- Install and configure Remote Access Service (RAS) on a Windows NT Server and manage RAS.
- Administer a Windows NT server by creating and managing accounts, security policies, system policies and user profiles.

**COURSE LENGTH:** 6 - 8 hour(s)

### **Unit Names:**

Unit 1: Identify the functions of the Gateway Service for NetWare (GSNW) Tool

Objectives:

- Install Gateway Service for NetWare on a Windows NT Server.
- Identify the advantages of the Migration Tool for NetWare.
- Identify the issues involved in migrating from a NetWare server to a Windows NT server.
- Migrate from a NetWare server to a Windows NT server using the Migration Tool for NetWare.
- Install File and Print Services for NetWare (FPNW) on a Windows NT server from an installation disk.
- Install Directory Service Manager for NetWare (DSMN) on a Windows NT Server from an installation disk.

Unit 2: Remote Access Service

Objectives:

- Install Remote Access Services (RAS) after setting up Windows NT Server 4.0.
- Configure the Windows NT server for RAS communication with a specified server.



- Configure the RAS server to support clients using the TCP/IP protocol.
- Configure the RAS server to support clients using the NWLink IPW protocol.
- Configure the RAS server to support clients using the NetBEUI Protocol.
- Install Point To Point Tunneling Protocol on a RAS server.
- Configure the RAS server to enable PPTP filtering.
- Manage dialing RAS permissions.
- Configure the RAS server for callback security.
- Configure the RAS Server for encryption.
- Sequence the steps for authenticating a remote user of the RAS server by using the security host.

### Unit 3: Administering a Windows NT Server

#### Objectives:

- Create a user account by using the New User menu option in the User Manager for Domains window.
- Assign a home directory to a user on the user's local drive.
- Disable a user account in a network.
- Unlock a user account in a network.
- Manage a local group account.
- Manage a local group membership.
- Set an account policy for a domain.
- Manage user rights.
- Assign a right to a user.
- Revoke a right from a user.
- Set the Audit policy of a domain to audit changes in the user account database.
- Set a Trust Relationships policy to enable users in a given domain to access resources in another domain.
- Identify the functions of system policies.
- Set a new system policy for all users in a group.
- Create a user profile for a user or group.
- Manage user profiles.
- Copy profile information to a network folder.
- Assign a profile path to a user account.



**Networking Technologies Series: TCP/IP Internetwork Management**

Course 12773

*Produced by NETg*

**LEARN TO:**

- Examine the services and protocols available in the Internet.
- Examine the properties of the LAN and WAN protocols that enable them to work with TCP/IP.
- Examine the components of Domain Name Service and the features of BOOTP and the Network Time Protocol.
- Examine the features of NFS and NIS.
- Examine the concepts of network management, network topologies, SNMP and MIB.

**COURSE LENGTH:** 6 - 8 hour(s)

**Unit Names:**

Unit 1: Internet

Objectives:

- Identify the features of an e-mail application.
- Identify the steps in the transmission of an e-mail.
- Identify the benefits of relaying mail.
- Sequence the command and responses between the sender and the receiver in Simple Mail Transfer Protocol (SMTP).
- Identify the ways by which MIME messages are sent by using ESMTP.
- Identify the services provided by Post Office Protocol (POP).
- Identify the benefits provided by Internet Message Access Protocol (IMAP).
- Identify the services provided by Network News Transfer Protocol (NNTP).
- Identify the features of Gopher.
- Identify the features of the WWW.

## NMCI Security Policy

- Sequence the components of an URL.
- Identify the features of HTML documents.

## Unit 2: TCP/IP and Networks

### Objectives:

- Identify the layers and services in a LAN that separates the IP layer from the Ethernet layer.
- Identify the properties of NetBIOS that enables it to operate with TCP/IP.
- Identify the protocols used by XNS which enables it to operate with TCP/IP.
- Identify the properties of IPX which enables it to operate with IP.
- Identify the features that enables ARCnet to operate with IP.
- Identify the properties of FDDI that enables it to operate with TCP/IP.
- Identify the method by which X.25 operates with IP.
- Identify the method by which ISDN operates with IP.
- Identify the method by which SMDS operates with IP.
- Identify the properties of ATM which enable it to operate with TCP/IP.
- Identify the layers of the Windows 95 architecture that enables it to work with TCP/IP.
- Match the TCP/IP services with their descriptions.

## Unit 3: Domain Name Service

### Objectives:

- Match the Internet domains with their descriptions.
- Identify the functions of a name server.
- Match the fields of a resource record with their descriptions.
- Identify the features of IN-ADDR-ARPA format.
- Match the fields of a DNS message with the information contained in them.
- Identify the different methods by which the name resolver resolves a name.
- Identify the features of the BOOTP protocol.
- Match the fields of the BOOTP message format with their descriptions.
- Match the fields of the Network Time Protocol(NTP) with their definitions.

## Unit 4: NFS and NIS

### Objectives:

- Identify the features of Network File System(NFS).
- Identify the features of Remote Procedure Call (RPC).
- Identify the function of External Data Representation (XDR).
- Identify the features of the Network Files System Protocol (NFSP).
- Match the mount protocol procedures with their descriptions.
- Identify the daemon processes involved in file locking.
- Identify the features of Remote Execution Service(REX).
- Identify the functions of rusers and rsh.
- Identify the features of Network Information System (NIS).

#### Unit 5: Managing TCP/IP

##### Objectives:

- Match the parts of network management with their descriptions.
- Identify the features of the SNMP network management standard.
- Identify the network expansion component to be used in a given topology.
- Identify the features of SNMP.
- Match the Management Information Base (MIB) fields with their descriptions.
- Match the SNMP commands with their descriptions.
- Identify the features of SNMP v1.

**Internetworking Microsoft TCP/IP on Microsoft Windows NT 4.0 - Part 1**

Course 71435

*Produced by NETg*

**LEARN TO:**

- Implement Microsoft TCP/IP on Microsoft Windows NT 4.0.
- Identify the installation procedure and the interface of Microsoft Network Monitor.
- Identify the methods in which the protocols in each of the four layers of the TCP/IP protocol suite work internally and in association with other protocols.
- Identify IP addressing principles and problems and assign IP addresses to hosts on a LAN environment.
- Define a subnetting and supernetting scheme based on a scenario.

**COURSE LENGTH:** 6 - 8 hour(s)

**Unit Names:**

Unit 1: Introduction to TCP/IP

Objectives:

- Identify the milestones in the history of TCP/IP.
- Identify the advantages of adding Microsoft TCP/IP to a Windows NT configuration.
- Identify the definitions and responsibilities of the Internet Society and Internet Architecture Board (IAB).
- Identify the definition of Request for Comments (RFC) document and its features.
- Identify the functions of the data transfer utilities of TCP/IP.
- Identify the functions of the remote execution utilities of TCP/IP.
- Identify the functions of the printing utilities of TCP/IP.
- Match the diagnostics utilities of TCP/IP with their functions.
- Install TCP/IP on Windows NT 4.0.

- Configure TCP/IP manually to support multiple network adapters.
- Test a TCP/IP configuration by using the diagnostics utilities IPCONFIG and PING.
- Install the full version of Microsoft Network Monitor on a Windows 95 client.
- Identify the data displayed by the panes on the Network Monitor Capture Summary Window of Network Monitor.

## Unit 2: TCP/IP Protocol Suite

### Objectives:

- Define the architecture of the Microsoft TCP/IP protocol suite.
- Sequence the steps in which the hardware address of a host is obtained by Address Resolution Protocol (ARP) in the address resolution process.
- Sequence the steps in which Address Resolution Protocol (ARP) resolves an IP address to a hardware address on a local network.
- Sequence the steps in which ARP allows two hosts on different networks to communicate.
- Display the entries in the ARP cache.
- Add an ARP entry to the ARP cache.
- Match the fields of an ARP packet with their functions.
- Identify the definition and function of Internet Control Message Protocol (ICMP).
- Identify the definition and function of Internet Group Management Protocol (IGMP).
- Match the fields of an IP datagram with their functions.
- Sequence the steps that the Internet Protocol (IP) performs when it receives a data packet from a router.
- Match the fields of an IP packet with their features.
- Identify the features of the connectivity slots supported by TCP/IP on Windows NT 4.0.
- Identify the features of Transmission Control Protocol (TCP).
- Identify the definition and purpose of TCP three-way handshake.
- Sequence the steps in which TCP sliding windows buffer the data for transmission between two hosts.
- Match the fields of a TCP header with the data they display.
- Identify the features of User Datagram Protocol (UDP).

## Unit 3: IP Addressing

### Objectives:

- Identify the features of the dotted decimal notation of an IP address.

- Match the binary formats of the IP addresses with their decimal values.
- Match the address classes with the types of network they accommodate.
- Match the address classes supported by TCP/IP with the IP addresses.
- Identify the guidelines for assigning network IDs and host IDs in a Windows NT 4.0 environment.
- Identify the regulations for assigning network IDs to network components.
- Identify the guidelines for assigning host IDs to network components.
- Match the IP addressing problems with their possible effects.
- Identify the features of default subnet masks that are used when networks are not divided into subnets.
- Identify the features of IP addressing with IP version 6.

#### Unit 4: Subnetting and Supernetting

##### Objectives:

- Identify the benefits of implementing subnetting with TCP/IP in a Windows NT 4.0 environment.
- Identify the steps that are performed before subnetting is implemented on a network.
- Identify the definition of subnet mask bits.
- Identify the steps in the process of defining a subnet mask.
- Given a network situation, identify the best subnetting configuration.
- Sequence the steps in the process of defining subnet IDs for an internetwork.
- Sequence the steps in which the number of hosts in each subnet is determined.
- Identify the function of the Classless Inter-Domain Routing (CIDR) technique used in supernetting.



**Internetworking Microsoft TCP/IP on Microsoft Windows NT 4.0 - Part 2**

Course 71436

*Produced by NETg*

**LEARN TO:**

- Identify the static and dynamic routing process.
- Implement routing and manipulate static entries in a routing table.
- Install and configure DHCP.
- Rectify DHCP configuration errors, manage the DHCP database and create a DHCP relay agent.
- Identify the definition of NetBIOS and NetBIOS names.
- Identify the functions and advantages of WINS.

**COURSE LENGTH:** 6 - 8 hour(s)

**Unit Names:**

Unit 1: Implementing IP Routing

Objectives:

- Identify the process of IP routing.
- Identify the features of static IP routing.
- Identify the features of dynamic IP routing.
- Identify the features of Routing Information Protocol.
- Identify the limitations of Routing Information Protocol.
- Identify the activities that need to be performed to integrate static and dynamic routing.
- Configure a Windows NT computer to act as a Windows NT router.
- Display the route a packet takes to reach its destination using the TRACERT utility.

- Identify the components of a routing table.
- Display the entries in a routing table.
- Remove the default gateway address from a routing table.
- Add a static routing table entry for a router using the ROUTE utility.
- Restore the address for the default gateway in the local routing table.
- Test the configured default gateway address by displaying the contents of the routing table.

## Unit 2: Fundamentals of DHCP

### Objectives:

- Identify the function of Dynamic Host Configuration Protocol (DHCP).
- Identify the differences between manually configuring TCP/IP and dynamically configuring TCP/IP using DHCP.
- Match the four phases DHCP uses to configure a DHCP client with the activities that occur in them.
- Identify the features of the IP lease request and offer phases.
- Identify the features of the IP lease selection and acknowledgement process.
- Identify the activities in the IP lease renewal process.
- Identify the guidelines for configuring IP addresses for allocating to clients in a multiple DHCP environment.
- Identify the implementation considerations for installing DHCP.
- Identify the requirements for implementing DHCP.
- Determine the network adapter card address from the DHCP server.
- Install the DHCP Server Service on the DHCP server.
- Create a DHCP scope that consists of one IP address with an assigned lease time of one day.
- Configure a DHCP scope option that automatically assigns a default gateway address to DHCP clients.
- Add a reservation for a client from the DHCP server.
- Test the DHCP server configuration by starting the DHCP client.

## Unit 3: Advanced Operations on DHCP

### Objectives:

- Display the DHCP server listing of leased addresses on the DHCP server.
- Renew the DHCP lease assigned to the DHCP client computer.

- Stop the Microsoft DHCP Server service to prevent address lease assignments and renewals.
- Display the result of an attempt to renew a lease when the DHCP server is unavailable.
- Release the IP address lease assigned to the DHCP client computer by using the IPCONFIG utility.
- Start Microsoft DHCP Server service to allow IP lease assignments and renewals.
- Reconfigure the DHCP Server to stop and start up the DHCP Server service manually.
- Reconfigure a DHCP client to use a static IP address by changing the configuration information.
- Restore the DHCP database manually using Regedit.
- Compact the DHCP database using the JETPACK utility.
- Identify the definition of DHCP relay agent.
- Install DHCP relay agent on a computer on a subnet.
- Start the Network Monitor to capture DHCP packets on a DHCP client.
- Install the DHCP client on a computer on a subnet which is not a designated DHCP relay agent.
- Disable the DHCP relay agent from a DHCP relay computer.
- Configure the DHCP relay computer to use a static IP address.

#### Unit 4: NetBIOS Over TCP/IP

##### Objectives:

- Identify the definition of NetBIOS, features of the NetBIOS utilities and NetBIOS scope ID.
- Match the NetBIOS processes with the activities that occur in them.
- Identify the features of the NetBIOS scope.
- Sequence the steps for resolving local NetBIOS names by using a broadcast.
- Identify the functions of the NBSTAT utility.
- Sequence the steps for resolving NetBIOS names by using a NetBIOS name server.
- Sequence the steps for resolving NetBIOS names using Microsoft methods.
- Match the NetBIOS over TCP/IP name resolution nodes with their functions.
- Identify the definition of the LMHOSTS file.
- Resolve a remote computer name by using a local broadcast.
- Configure LMHOSTS to resolve a remote NetBIOS computer name at the command prompt.
- Resolve NetBIOS names by using the NetBIOS name cache.

#### Unit 5: Implementing Windows Internet Name Service

Objectives:

- Identify the functions of WINS.
- Identify the steps used to resolve a NetBIOS name to an IP address.
- Identify the advantages of WINS.
- Identify the phases used to resolve a NetBIOS name.
- Sequence the steps in the NetBIOS name registration with a WINS server.
- Sequence the steps in the lease renewal of a NetBIOS name with a WINS server.
- Identify the steps in the NetBIOS name release from a WINS server.
- Sequence the steps in resolving a NetBIOS name to an IP address by using a WINS server.
- Identify the considerations for implementing WINS in an internetwork.
- Identify the procedures for implementing WINS.
- Install a WINS server.
- Start the DHCP Server service.
- Assign WINS server address by using DHCP Manager.
- Renew the DHCP lease of a client at the command prompt.
- Resolve a NetBIOS name.
- Configure a static mapping for a non-WINS client by using WINS Manager.
- Configure a WINS proxy agent.
- Remove the WINS proxy agent.

**Internetworking Microsoft TCP/IP on Microsoft Windows NT 4.0 - Part 3**

Course 71437

*Produced by NETg*

**LEARN TO:**

- Administer a WINS environment by configuring database replication between WINS servers and maintaining the WINS server database.
- Identify the working of the Windows NT browsing service.
- Resolve a host name to an IP address by using different Microsoft supported methods.
- Identify the structure and components of the domain name system.

**COURSE LENGTH:** 6 - 8 hour(s)

**Unit Names:**

Unit 1: Administering a WINS Environment

Objectives:

- Configure a WINS server to automatically remove obsolete entries from the WINS database.
- Match the advanced WINS server configuration options with their actions.
- Delete a WINS server from the WINS database.
- Identify the methods of replicating the WINS database.
- Configure a WINS server as a push partner.
- Maintain the WINS database by using the WINS Manager utility to sort the mappings by IP address.
- Add a static mapping to the WINS database for resolving host name for a non-WINS enabled computer.
- Make a backup of the WINS database.
- Make a backup of the WINS Registry entries.

## NMCI Security Policy

- Restore the backup copy of the WINS database.
- Compact the WINS database using the JETPACK utility.

### Unit 2: IP Internet Browsing and Domain Functions

#### Objectives:

- Identify the functions of the different computers participating in the browsing service.
- Sequence the steps followed by the computer browsing service for servicing client browsing requests.
- Identify the advantages of the LMHOSTS file.
- Configure a Windows NT client with the WINS browsing.
- Identify the additional functions of Windows NT browsing services.

### Unit 3: Host Name Resolution Methods

#### Objectives:

- Identify the uses of a host name.
- Sequence the steps for resolving the host names by using the HOSTS file method.
- Sequence the steps for resolving the host names by using the DNS server method.
- Sequence the steps for resolving the host names by using the Microsoft-supported methods.
- Configure the HOSTS file for resolving host names by adding a host name and the IP address mapping to the HOSTS file.
- Configure the Windows NT server to use a DNS server for resolving host names.

### Unit 4: Domain Name System

#### Objectives:

- Identify the definition of DNS.
- Match the components of the domain name space structure with their features.
- Match the different DNS servers with their functions.
- Match the DNS files with their functions.
- Identify the various types of queries.
- Sequence the steps followed by a name server in caching resolved queries.

**Internetworking Microsoft TCP/IP on Microsoft Windows NT 4.0 - Part 4**

Course 71438

*Produced by NETg*

**LEARN TO:**

- Install the DNS Server.
- Configure and manage the DNS Server.
- Identify the connectivity requirements for Microsoft networking.
- Identify the purpose of the printing utilities for TCP/IP.
- Identify the basic concepts of SNMP and manage the SNMP service.
- Identify the common characteristics of TCP/IP-related problems and functions of Windows NT diagnostic tools.

**COURSE LENGTH:** 6 - 8 hour(s)

**Unit Names:**

Unit 1: Domain Name System Implementation

Objectives:

- Install the DNS Server service on a Windows NT Server.
- Identify the features of DNS zones.
- Set up a primary zone on a primary DNS Server.
- Add a resource for a zone.
- Match the NSLOOKUP command options with their purposes.
- Sequence the steps in the process by which a DNS client obtains an IP address from a WINS Server.
- Add an alias for a host in a DNS zone.
- Configure WINS host name resolution for a zone.
- Configure WINS reverse lookup resolution for a reverse lookup zone.

## Unit 2: Connectivity in Heterogeneous Environments

### Objectives:

- Identify the connectivity requirements for Microsoft networking.
- Given a situation, identify the appropriate command to execute commands on a Unix host.
- Install the Internet Information Server (IIS) to access the File Transfer Protocol (FTP) service on a Windows NT server.
- Given a situation, identify the appropriate command to transfer data to or from a remote host.
- Identify the benefits of the types of data transfer utilities.
- Identify the purpose of the printing utilities for TCP/IP.
- Set up the TCP/IP Print Server service on a Windows NT computer.
- Install a TCP/IP printer on a Windows NT computer that will manage the printer settings on a network.
- Manage a TCP/IP printer.

## Unit 3: Implementing the Microsoft SNMP Service

### Objectives:

- Identify the features on the SNMP protocol.
- Match the management information bases (MIBs) supported by SNMP with their features.
- Identify the functions of the Microsoft SNMP service.
- Identify the features of an SNMP community.
- Install SNMP service on a Windows NT computer.
- Configure SNMP agent services on a Windows NT computer.
- Verify communications between the SNMP service and SNMP management systems by using the SNMPUTIL utility.
- Sequence the steps by which the SNMP service processes information requests from management systems.

## Unit 4: Troubleshooting Microsoft TCP/IP

### Objectives:

- Match the TCP/IP-related problems with their common characteristics.
- Match the Windows NT diagnostic tools with their functions.
- Sequence the objects on which the PING utility is run to verify IP communication.
- Identify the methods to verify TCP/IP session communication.





## **Microsoft Exchange Server 5.5 Design and Implementation - Part 1**

Course 73365

*Produced by NETg*

### **LEARN TO:**

- Identify the features of shared-file messaging systems and client/server messaging systems.
- Identify the core and additional components of the Exchange Server.
- Analyze the network and messaging needs of an organization to enable you to design a server, site and user placement plan for an organization.
- Identify the preparations required before the installation of Exchange Server 5.5.

**COURSE LENGTH:** 6 - 8 hour(s)

### **Unit Names:**

Unit 1: Exchange Server: Introduction

Objectives:

- Identify the features of the shared-file messaging systems.
- Identify the features of the client/server messaging systems.
- Identify the software requirements for a given network environment to coexist with Exchange Server.
- Match the various organizational units in an Exchange Server hierarchy with their features.
- Identify the Windows NT security features integrated with the Exchange Server.
- Identify the features of the Microsoft Outlook client.

Unit 2: Exchange Server Architecture

Objectives:

- Match the core components of Exchange Server messaging infrastructure with their functions.

- Match the additional components of Exchange Server messaging infrastructure with their functions.
- Identify the functionality provided by the core components of Exchange Server when they communicate with other components.
- Identify the functionality provided by the Administrator Program when it communicates with other components.
- Identify the functionality provided by the communication between the clients and the core components.
- Identify the functionality provided by the additional components of Exchange Server when they communicate with other components.
- Sequence the steps for a single-server message flow between clients.

### Unit 3: Exchange Server Organizational Design

#### Objectives:

- Identify the guidelines to be considered in an Exchange Server Organization planning process.
- Identify the network topology guidelines for planning the design of a Microsoft Exchange Server Organization.
- Identify the conditions when defining site boundaries.
- Identify how users need impact the design process.
- Identify the most appropriate server hardware design plan in a given situation.
- Identify organizational requirements that are best satisfied by a specific arrangement of servers.
- Match the appropriate connectors with the scenarios.
- Match the client connection options available when designing an Exchange Server messaging system with their features.
- Select the appropriate designation of additional Exchange Server roles in a given scenario.
- Match the naming guidelines used for each object in a Microsoft Exchange Organization with the Organization object.
- Match the correct E-Mail address to be generated for communicating with a specific foreign messaging system.

### Unit 4: Installing Exchange Server

#### Objectives:

- Identify the installation requirements for Exchange Server.
- Match the various Windows NT account permissions with their functional benefits.
- Identify when you would use each installation option for Exchange Server 5.5 installation.

- Install Exchange Server 5.5 by using the CD-ROM.
- Create an Exchange Server mailbox.
- Identify the site-level administration features of the Exchange Administration Program.
- Configure organization permissions in an Exchange Server environment.
- Configure site permissions in an Exchange Server environment.
- Configure the configuration container permissions in an Exchange Server environment.
- Add an Exchange Server to an existing site.
- Identify the characteristics of a Microsoft Cluster Server environment.
- Identify the characteristics of the Exchange Server 5.5 upgrade process from a previous version.
- Execute Exchange Performance Optimizer by using the Microsoft Exchange Server program submenu.
- Match the folders created during installation with their contents.
- Match the Exchange Server services with their dependencies.

## **Microsoft Exchange Server 5.5 Design and Implementation - Part 2**

Course 73366

*Produced by NETg*

### **LEARN TO:**

- Understand the process of communication and information management between Microsoft Exchange servers in a site within a Microsoft Exchange organization.
- Identify the concepts in a multisite environment and configure Local Address space.
- Define X.400 and X.500 messaging recommendations, components of message handling systems, management domains and the role of interpersonal messaging systems.
- Manage a Site Connector and identify the functions of target server cost.
- Describe the features and benefits of the X.400 Connectors.

**COURSE LENGTH:** 6 - 8 hour(s)

### **Unit Names:**

#### Unit 1: Intrasite Server Communication

##### Objectives:

- Identify the features of intrasite server communication.
- Identify how RPC traffic over a WAN within a site affects network performance.
- Identify the functions of the MTA in intrasite server communication.
- Sequence the steps in the MTA process when data is transferred between two MTAs.
- Identify the functions of MTA Associations.
- Distinguish between the types of addresses used by Microsoft Exchange Server.
- Sequence the steps that the MTA follows to route information.
- Sequence the steps of the Directory Service process.
- Identify the communication tasks performed by the Information Store.

- Identify the functions of the System Attendant.
- Match the types of intrasite communication connectors with their functions.
- Identify the functions of Mail Directory Synchronization service.
- Sequence the steps for adding a server to a site.
- Identify the functions of the Knowledge Consistency Checker (KCC).
- Sequence the steps performed by the KCC to compare information contained in servers within a site.
- Sequence the events used by servers to maintain up-to-date directory information.

## Unit 2: Intersite Server Communication

### Objectives:

- Identify the features of a multiple site environment.
- Identify the function of the types of connectors.
- Identify the features of an address space.
- Configure address space by using the Site Connector Properties page.
- Identify the uses of assigning costs to a connector.
- Identify the most appropriate routing path for a message given the cost of the connectors.
- Match the options on the Schedule property page with the situations in which their selection is appropriate.
- Configure the Delivery Restrictions by using the Delivery Restrictions property page.
- Match the rights on the Permissions property page with their functions.
- Match the options on the Connected Sites property page with their functions.

## Unit 3: X.400 and X.500 Concepts

### Objectives:

- Identify the advantages of conforming to the X.400 standard.
- Match the components of X.400 MHS with the services they provide.
- Identify the features of types of management domains of X.400.
- Identify the features of X.500 recommendation.
- Identify the limitations of the X.500 recommendations.
- Sequence the steps followed by the MTS for message delivery when a user submits a message to the MTS.
- Identify the features of the two basic components of an X.400 message.

- Match the type of O/R addresses with their delivery mechanism.
- Distinguish the types of information objects provided by the interpersonal messaging system.
- Distinguish the contents of the two types of IPM structure components.
- Identify the purpose of the types of interpersonal notification conveyed between IPMS users.

#### Unit 4: Site Connector

##### Objectives:

- Identify the benefits of a Site Connector.
- Identify the functions of the server configuration options used for configuring a Site Connector.
- Identify the uses of the target server cost.
- Identify the security considerations for maintaining the Site Connector security.
- Match the different options on the General property page with their functions.
- Match the configuration options on the Target Servers property page with their functions.
- Match the options on the Address Space property page with their functions.
- Establish a connection with a remote site by filling the fields in the Override property page.
- Establish a connection between two Microsoft Exchange Server sites by creating a Site Connector.
- Verify the addition of a Site Connector by displaying the routing table.
- Remove a site connector by using Microsoft Exchange Administrator.
- Regenerate the routing table by using Microsoft Exchange Administrator.

#### Unit 5: X.400 Connector

##### Objectives:

- Identify the features of the X.400 Connector.
- Identify the benefits of using the X.400 Connector.
- Identify the features of MTA transport stack.
- Identify the functions of TP4 protocol.
- Configure the X.400 Connector by specifying general information in the General property page.
- Configure the X.400 Connector by specifying transport address information in the Stack property page.
- Configure the X.400 Connector by changing the default MTA attributes in the Override property page.

- Configure the X.400 Connector by specifying the advanced information in the Advance property page.
- Install the TP4/CLNP networking software on your computer running Windows NT.
- Install the TP4 MTA transport stack by using the Microsoft Exchange Administration program.
- Configure a new X.400 Connector to use the TP4 MTA Transport Stack.



## **Microsoft Exchange Server 5.5 Design and Implementation - Part 3**

Course 73367

*Produced by NETg*

### **LEARN TO:**

- Identify the functions and configure a Dynamic RAS connector.
- Identify selection and routing mechanisms used by the MTA to transfer a message across a connector.
- Understand the process of Directory Replication between sites and various methods of administering Directory Replication.
- Create a Public Folder, send mail to it and set up the visibility of the Public Folders.

**COURSE LENGTH:** 6 - 8 hour(s)

### **Unit Names:**

#### Unit 1: Dynamic RAS Connector

##### Objectives:

- Identify the functions of a Dynamic RAS Connector.
- Define an MTA transport stack for creating a Dynamic RAS Connector.
- Configure the directory and transport information by using the General tab.
- Provide authentication credentials to connect to a remote site by using the RAS Override page.
- Create an address space for routing a message on a Dynamic RAS connector by using the given RAS properties dialog box.
- Identify the special configuration options when using RAS with TCP/IP.

#### Unit 2: Multisite Message Routing and Selection

##### Objectives:

- Identify the role of the MTA in routing a message through multiple connectors.

- Identify the availability of a connector for a given situation.
- Interpret the given address from a Gateway Address Routing Table of a site.
- Configure a connector of one site with the bridgehead server on another site.
- Verify the connection between two sites connected by a Site Connector by using the MailStorm utility.
- Identify the selection criteria used by an MTA to select the best connector for delivering a message.
- Sequence the steps performed by an MTA for rerouting of a message in a multiple connector environment.
- Identify the functions of a Routing Calculation Server in routing a message.

### Unit 3: Directory Replication

#### Objectives:

- Identify the tasks for establishing Directory Replication between sites.
- Identify the possibility of directory replication between two sites in an existing message routing topology.
- Identify the most efficient Directory connector topology that results in minimum delays of replication information across sites.
- Configure directory Replication connector by using the Microsoft Exchange server Administrator program.
- Identify the functions of Knowledge Consistency Checker (KCC).
- Match the processes that manage Directory Replication between sites with their importance.
- Sequence the order of events during the configuration of Directory Replication between three sites.
- Identify the reasons to force Directory Replication from a specific inbound site.

### Unit 4: Public Folders Replication

#### Objectives:

- Identify the features of the Public Folder components.
- Set up the visibility of a Public Folder in the global address list by using the Microsoft Exchange Administrator program.
- Create a Public Folder by using Microsoft Outlook.
- Send mail to a Public Folder by using the menu bar.
- Configure Public Folder replication by using the Replicas property page.
- Match the message attributes used to monitor message state information with their features.

- Sequence the steps in which the message modifications are replicated across various Information Stores.
- Identify the events that take place during the various types of Public Folder conflicts.
- Identify the situations in which the out-of-sync Public Folders can resynchronize by using the backfill process.
- Rehome a Public Folder by using the Microsoft Exchange Server Administrator program.

**Microsoft Exchange Server 5.5 Design and Implementation - Part 4**

Course 73368

*Produced by NETg*

**LEARN TO:**

- Identify the protocols used, the messages and security measures associated with Exchange Server and the Internet.
- Install and configure Internet Mail Service.
- Identify the components of USENET network.

**COURSE LENGTH:** 6 - 8 hour(s)

**Unit Names:**

Unit 1: Exchange Server With the Internet

Objectives:

- Match the Exchange Server supported Internet protocols with their usage.
- Identify the levels at which Internet protocols should be configured in a given situation.
- Configure Internet protocols at the mailbox level by using the Protocols property sheet.
- Enable Protocol Logging for Internet protocols by using Registry Editor.
- Match the performance counters for Internet protocols with the keys under which they appear in the Performance Monitor.
- Identify the functions of the MIME type Internet messages.
- Identify the TCP/IP ports configuration for given situations.
- Sequence the steps in the DNS name resolution process.
- Match the different security methods associated with Exchange Server and the Internet with their descriptions.

Unit 2: Internet Mail Service (IMS)

### Objectives:

- Sequence the steps involved in the flow of an outbound message in the IMS process.
- Sequence the steps involved in the SMTP process.
- Sequence the steps involved in a successful ESMTP connection.
- Identify the security features that are supported by IMS to provide greater security than basic authentication.
- Identify the advantages of using multiple IMSs.
- Set up a site by modifying the SMTP address.
- Install IMS by using Internet Mail Wizard.
- Match the options available on the Internet Mail property sheet with their functions.
- Match the options available on the Dial-up Connections property sheet with their functions.
- Match the options available on the Connections property sheet with their functions.
- Match the options available on the Queues property sheet with their functions.
- Match the options available on the Routing property sheet with their functions.
- Enable secure outbound connections to other Exchange Server computers.
- Identify the functions of the General property sheet.
- Identify the functions of the Address Space property sheet.
- Configure the IMS by setting the scope for restricting address space.
- Sequence the steps involved in an ETRN session.
- Add an e-mail domain to the server on which the IMS is installed by using ETRN.
- Dequeue an e-mail message by using the ETRN command.
- Test IMS by using the Telnet Utility.
- Send a test message to another Organization by using the Microsoft Outlook utility.
- Display the routing table for a server in another site.
- Display the DNS MX record for an Organization.

### Unit 3: Internet News Service (INS)

#### Objectives:

- Identify the features of USENET newsgroups.
- Identify the functions of the INS.
- Match the components of USENET network with their description.
- Differentiate between a push feed and a pull feed.
- Sequence the steps involved in a typical push feed session.

- Sequence the steps involved in a typical pull feed session.
- Create the INS newsfeed object by using the Newsfeed Configuration Wizard.
- Create a public folder by using Microsoft Outlook.
- Post a message into a subfolder by using Microsoft Outlook.
- Publish a public folder as a newsgroup by using Exchange Administrator window.
- Grant anonymous users the Nonediting Author role on a subfolder by using Microsoft Outlook.
- Match the options on the General property sheet with their functions.
- Match the options on the Messages property sheet with their functions.
- Match the options on the Hosts property sheet with their functions.
- Match the options on the Connections property sheet with their functions.
- Match the options on the Security property sheet with their functions.
- Match the options on the Advanced property sheet with their functions.
- Match the icons in the Inbound property sheet with what they indicate.
- Match the icons in the Outbound property sheet with what they indicate.
- Configure a pull feed by using the Newsfeed Configuration Wizard.
- Publish a message in a public folder by using Microsoft Outlook.
- Enable anonymous client access by using Exchange Server Administration Program.
- Test the INS by using Telnet.
- Identify the different tools for troubleshooting INS.
- Match the property sheets on the NNTP object with their functions.
- Match NNTP commands with their functions.
- Match the NNTP control messages with their functions.

## **Microsoft Exchange Server 5.5 Design and Implementation - Part 5**

Course 73369

*Produced by NETg*

### **LEARN TO:**

- Identify the POP3 and IMAP4 features and functionality.
- Identify the POP3 and IMAP4 authentication methods, configuration options and troubleshooting methods.
- Configure and verify POP3 and IMAP4 client functionality.
- Identify the LDAP features, functionality and operation.
- Identify the property pages used to configure LDAP and configure an Outlook Express client to access Exchange Server Directory Service using LDAP.
- Identify the features of Outlook Web Access and the steps in the information flow to exchange messages using Outlook Web Access.
- Install and configure Outlook Web Access.
- Access Exchange Server public folders and a mailbox by using Internet Explorer 4.

**COURSE LENGTH:** 6 - 8 hour(s)

### **Unit Names:**

Unit 1: Internet Protocols: POP3 and IMAP4

Objectives:

- Identify the functions of POP3 commands.
- Sequence the steps in an Exchange Server POP3 session.
- Identify the functions of IMAP4 commands.
- Identify the steps in the IMAP4 message transfer process.
- Sequence the steps in an Exchange Server IMAP4 session.
- Match the POP3 and IMAP4 user authentication types with their features.
- Sequence the steps in the NTLM authentication process.

- Sequence the steps in the SSL encryption process.
- Identify the configuration options available for enabling Internet mail protocol objects.
- Identify the property pages used to set the protocol configuration options.
- Enable the Internet mail protocol for a mailbox.
- Configure an Outlook Express client to be used with Internet mail access protocols.
- Verify message delivery from a client to the Information Store by using Outlook Express.
- Enable protocol logging by using the Windows NT Registry Editor.
- Verify the POP3 functionality by using Telnet.
- Verify the IMAP4 functionality by using Telnet.
- Display the Internet mail protocol log file by using the Windows NT Explorer.

## Unit 2: Internet Protocol: LDAP

### Objectives:

- Identify the features of LDAP.
- Identify the LDAP commands that are supported by Microsoft Exchange Server.
- Sequence the steps in an Exchange Server LDAP session.
- Identify the property pages that are used to set LDAP configuration options.
- Configure an Outlook Express client to access the Exchange Server Directory Service using LDAP.
- Resolve a display name in a new message by using LDAP.

## Unit 3: Outlook Web Access

### Objectives:

- Identify the features of the core technologies on which the Active Platform is based.
- Match the components used by Outlook Web Access with their functions.
- Identify the functions of the Collaboration Data Objects (CDO) libraries.
- Sequence the steps involved in the information flow process to access an Exchange Server mailbox from a Web browser.
- Sequence the steps involved in the authentication process to access an Exchange Server mailbox from a Web browser.
- Install Outlook Web Access by using the Microsoft Exchange Server Setup program.
- Identify the property pages used to set HTTP (Web) configuration options.
- Configure the HTTP (Web) Site Settings object to enable anonymous users to access public



folders.

- Anonymously access the Exchange Server public folders by using Internet Explorer 4.0.
- Access an Exchange Server mailbox by using Internet Explorer 4.0.

**Networking Technologies Series: Managing Multivendor Networks**

Course 12763

*Produced by NETg*

**LEARN TO:**

- Describe the benefits and challenges to integration.
- Describe the standards for integration.
- Define multivendor terminology.
- Identify components of internetworking.
- Identify the steps used to provide interoperability between heterogeneous software applications.
- Identify client/server considerations.
- Identify client/server models.
- Identify network management problems.
- Identify the functions of the network management model.
- Identify network security issues.

**COURSE LENGTH:** 6 - 8 hour(s)

**Unit Names:**

Unit 1: Integrating Multivendor Networks

Objectives:

- Identify the benefits of an integrated network.
- Identify the challenges in multivendor network integration.
- Match the terms used in multivendor network integration with their definitions.
- Match the related terms used in multivendor network integration with their definitions.
- Identify the functions of the three layers of the communication model used in integration.
- Identify the reasons for using an integration blueprint for successful integration.

- Identify the benefits of using the two types of open system specifications.
- Identify the characteristics of the two types of proprietary specifications, NetBIOS and SPX/IPX.
- Match the protocol integration methodologies used to build an integrated network with their features.

## Unit 2: Internetworking and Interoperability

### Objectives:

- Identify the guidelines to select internetworking components.
- Identify the services provided by a repeater.
- Identify the features of bridges.
- Identify the features of routers.
- Identify the functions of a gateway.
- Identify the tasks that can be performed by providing interoperability across a network.
- Identify the services provided by the remote terminal access solutions.
- Identify the characteristics of remote program execution.
- Identify the characteristics of the store-and-forward interoperable file transfer system.
- Identify the features of the NFS distributed file system solution.
- Identify the features of the e-mail integrating solutions, Lotus cc:Mail and Microsoft Mail.
- Identify the features of the modes of PC network integration, Peer-to-peer and File server based mode.
- Identify the functions of the interoperable database access solutions, Client-driven, Gateway-driven, and Database-driven.

## Unit 3: Client-Server Integration

### Objectives:

- Identify the services provided by the client/server environment.
- Identify the features of client/server solutions.
- Identify the features of the distributed presentation model.
- Identify the functions of the remote distribution model.
- Identify the features of the distributed function model.
- Identify the features of the remote data access model.
- Identify the features of the distributed database model.

#### Unit 4: Network Support and Management

##### Objectives:

- Identify the problems encountered in network management.
- Match the five layers of the OSI network management model with their associated activities.
- Match the three approaches to network management with their features.
- Match the components of the SNMP network management model with their features.
- Identify the security factors in the network.
- Identify the reasons for providing support services to networks.
- Identify the major areas of future trends in integration.

## **UNIX SVR4 System Administration Advanced Topics**

Course 12779

*Produced by NETg*

### **LEARN TO:**

- Monitor the performance of the UNIX system.
- Identify the process of implementing internet e-mail and sendmail in a UNIX environment.
- Administer a UNIX-to-UNIX Copy Program (UUCP) to enable effective communication between UNIX machines.
- Identify the possible security threats to a UNIX system and the methods used to make the system more secure.

**COURSE LENGTH:** 7 - 8 hour(s)

### **Unit Names:**

#### Unit 1: Performance Monitoring

##### Objectives:

- Display the number of processes in the UNIX run queue using the uptime command.
- Display a graphical report of the system status using the perfmeter tool.
- Display a report on the system status for a specified time interval using the sar command options.
- Monitor CPU and system performance using the commands provided by UNIX.
- Display a report on the multiprocessor performance using the mpstat command.
- Display the active processes in the system using the ps command.
- Identify the uses of the two UNIX memory management techniques.
- Display a report on the memory performance of the system for a specified time period using the vmstat command.
- Display a report on the system's utilization of its memory resources for a specified time interval using the sar command.

- Identify the hardware-oriented approaches to optimize system performance.
- Identify the guidelines to use relational databases on UNIX systems.
- Display the disk performance statistics for a specified time period using the iostat command.
- Display a report on the disk performance and I/O activity of the system for a specified time interval using the -d option of the sar command.
- Display the free disk space on each file system that is mounted using the df command.
- Identify the guidelines for kernel tuning.
- Match the kernel tables used in kernel tuning with their functions.
- Display the kernel tables for a specified time interval using the -v option of the sar command.
- Display tunable kernel parameters using the nm command.
- Display current values of tunable kernel parameters using the sysdef command.
- Modify the values of tunable kernel parameters in the configuration information file using the set command.

## Unit 2: Mail Administration

### Objectives:

- Identify the uses of the e-mail programs.
- Match the Request for Comments (RFC) documents with their functions.
- Identify the use of the two high-level transfer protocols, File Transfer Protocol (FTP) and Simple Mail Transfer Protocol (SMTP).
- Identify the steps involved in sending e-mail using the Domain Name System.
- Identify the features of MX records.
- Sequence the steps involved in sending mail from the client to the host using MX records.
- Identify the use of an envelope address.
- Identify the users of sendmail.
- Match the sendmail auxiliary files with their functions.
- Identify the uses of the configuration file.
- Declare the given aliases for an alias name.
- Sequence the steps involved in setting up sendmail.
- Create macros/classes using appropriate operators.
- Add a header definition to the configuration file using the H operator.
- Change the sendmail settings according to requirements, using the O operator.
- Set the delivery precedence of a class to a specified value, using the P operator.

## NMCI Security Policy

- Define a given key file in the sendmail configuration file using the K operator.
- Identify the function of the S and R operators.

### Unit 3: UUCP Administration

#### Objectives:

- Match the UNIX-to-UNIX Copy Program (UUCP) files with their uses.
- Match the various support file types with their features.
- Match the different daemons available in UUCP with their uses.
- Sequence the steps of initiating a system to receive UUCP calls.
- Match the fields that are edited in the Systems file with their contents.
- Sequence the role of chat scripts in data transfer.
- Test the UUCP connection using the Uutry command.
- Copy a file from one machine to another using the UNIX-to-UNIX Copy Program command.
- Run a specified command on a remote machine using the uux command.
- Display system function information using the two UUCP utilities.

### Unit 4: UNIX System Security

#### Objectives:

- Identify the threats to a UNIX system and the methods used to implement file security.
- Match the type of attacks on the UNIX system with their prevention measures.
- Identify the uses of the two methods used to prevent cracking reusable passwords.
- Identify the functions of the two methods used to implement one-time passwords.
- Select the guidelines for a good backup policy.
- Identify the features of FTP that can be used by crackers to attack a computer system.
- Identify the methods used to prevent illegal access to a computer system that uses sendmail.
- Identify the features of Network File System that can be used to crack a system.
- Identify the features of Trivial File Transfer Protocol (TFTP) that are used to gain illegal access to a system.
- Identify the feature of a message digest.
- Identify the uses of C2 auditing.
- Identify the uses of a program wrapper.
- Identify the use of the three security tools.
- Identify the functions of firewalls.

## NMCI Security Policy

- Identify the features of kerberos.
- Identify the use of dial-back modems.
- Identify the function of an encrypted Ethernet hub.
- Identify the features of a filtering router.



**Networking Technologies Series: Data Integrity**

Course 12765

*Produced by NETg*

**LEARN TO:**

- Identify the factors that affect data integrity.
- Identify the methods to improve data integrity and fault tolerance.
- Identify backup system components.
- Describe types of backup strategies.
- Identify the devices and media used to make a backup.
- Identify methods for archiving data
- Describe the structure and components of hierarchical storage management (HSM).
- Identify the characteristics of databases.
- Sequence the steps involved in disaster recovery methodology.

**COURSE LENGTH:** 6 - 8 hour(s)

**Unit Names:**

Unit 1: Data Integrity Issues

Objectives:

- Match the hardware problems with their effects on data integrity.
- Match the logical problems with their effects on data integrity.
- Match the techniques for preventing loss of data integrity with their functions.
- Match the corrective techniques used in data integrity with their functions
- Describe the common and the redundant methods used to improve fault tolerance.
- Match the commonly used methods to improve fault tolerance with the services they provide.
- Match the redundant methods used to improve fault tolerance with their functions.

## Unit 2: Network Backup Systems

### Objectives:

- Match the network backup systems with their features.
- Match the backup system components with their features.
- Identify the requirements, strategies and the backup system techniques.
- Identify the services that a backup system must provide.
- Choose a backup strategy.
- Match the backup techniques with their functions.
- Identify the features of tape and optical media used for making backups.
- Match the techniques used to improve backup performance with their features.
- Match the automated devices for making backups with their features.

## Unit 3: Archiving and Hierarchical Storage Management (HSM)

### Objectives:

- Identify the reasons for archiving data.
- Match the methods of archiving data with their features.
- Identify the methods to build redundancy for data in a storage medium.
- Match the components of HSM with their functions.
- Identify the features of the different hierarchical structures, two-tiered HSM system and three-tiered HSM system.
- Sequence the steps used by HSM to decrease the load on the network while archiving data.
- Identify the benefits of integrating the HSM and backup systems.

## Unit 4: Recovery of Data

### Objectives:

- Identify the characteristics of databases on a network.
- Match the database applications on LANs with their features.
- Identify the result of the backup operation.
- Identify the guidelines to be followed when preparing for disaster recovery methodology.
- Identify the different methods to prepare for disaster recovery.
- Sequence the steps involved in the disaster recovery methodology.

## **Implementing Security for Web Sites - Part 2**

Course 12701

*Produced by NETg*

### **LEARN TO:**

- Identify the various encryption methods.
- Recognize the steps of PGP key management.
- Identify the PGP configuration file.
- Understand the threats associated with the Web.
- Describe stages in the evolution of Java, its features, and security mechanisms.
- Recognize features of the Applet Viewer.
- Recognize security restrictions in Netscape Navigator 2.0.
- Identify the CGI security risks and the measures to minimize these risks.
- Recognize the various language issues related to CGI.
- Identify the types of viruses.
- Name the reasons for virus targets.
- Describe how antivirus programs work.
- Implement preventive measures and cures for viruses.

**COURSE LENGTH:** 7 - 8 hour(s)

### **Unit Names:**

Unit 1: Messaging Security

Objectives:

- Identify the features of the two methods of Encryption: Substitution and Transposition.
- Match the Substitution methods of encrypting data with their features.
- Identify the arrangement of data in Transposition.

## NMCI Security Policy

- Identify the need for PGP.
- Know the steps to use PGP.
- Understand the key management functions of PGP.
- Identify the reasons for using PGP.
- Match the commands for key management in PGP with their uses.
- Match the steps in working with PGP with their features.
- Understand the basic message operation of PGP.
- Match the components of advanced message operations in PGP with their uses.
- Identify the features of PGP configuration file, the various security measures and PGP add-ons.
- Match the chief configuration keywords and options with their uses.
- Match the various types of attacks on PGP with their appropriate security measures.
- Match the PGP add-ons with their functions.

## Unit 2: Java and Web Site Security

### Objectives:

- Identify the threats associated with the Web.
- Identify the risks associated with a Web clients and Web server.
- Identify the need for and features of the Java Virtual Machine.
- Learn about the stages in the evolution of Java.
- Describe the features of Java.
- Identify the security checks conducted by the bytecode verifier.
- Identify the functions of a class loader.
- Identify the features of Applet Viewer.
- Identify the security restrictions in Netscape Navigator 2.0.

## Unit 3: CGI and HTTP Security

### Objectives:

- Identify the features and security risk associated with CGI program.
- Identify the features of a CGI.
- Identify the various points of attacks in a CGI program.
- Identify the various measures and issues related to CGI and HTTP security.
- Minimize CGI security risks.

- Recognize the features of the CGI Wrap program.
- Match the Server Side Includes (SSI) tags with their functions.
- Identify the features of some CGI programming languages.
- Identify the steps to query a database on a separate server.

#### Unit 4: Viruses

##### Objectives:

- Identify the features of viruses.
- Identify the reasons for system components serving as targets for viruses.
- Identify the different types of viruses.
- Describe the features of boot record viruses.
- Identify the features of program file viruses.
- Identify the features of macro viruses.
- Identify the working of various classes of viruses.
- Analyze how polymorphic viruses operate.
- Analyze how stealth viruses operate.
- Examine how slow viruses work.
- Examine how retro viruses work.
- Understand how various antivirus programs work.
- Understand how virus scanners work.
- Understand how memory scanners work.
- Know how integrity checkers work.
- Describe how behavior blockers work.
- Know how heuristic scanners work.
- Name the measures that can be taken for the prevention and cure of viruses.
- Prevent viral infections.

